ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

EVALUATING USABILITY OF SECURITY MECHANISMS OF E-HEALTH APPLICATIONS: CASES FROM ETHIOPIA

By

ANTONYO GEORGE

JUNE 2020

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

EVALUATING USABILITY OF SECURITY MECHANISMS OF E-HEALTH APPLICATIONS: CASES FROM ETHIOPIA

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science and Systems (*Information Systems Specialization*)

By: **ANTONYO GEORGE**

Advisor: **LEMMA LESSA (Ph.D.)**

June 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

EVALUATING USABILITY OF SECURITY MECHANISMS OF E-HEALTH APPLICATIONS: CASES FROM ETHIOPIA

By: **Antonyo George**

Name and signature of Members of the Examining Board

Lemma Lessa (Ph.D.) Advisor	_____ Signature	_____ Date
Rahel Bekele (Ph.D.) Examiner	_____ Signature	_____ Date
Getachew Hailemariam (Ph.D.) Examiner	_____ Signature	_____ Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that this thesis entitled "EVALUATING USABILITY OF SECURITY MECHANISMS OF E-HEALTH APPLICATIONS: CASES FROM ETHIOPIA" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Antonyo George

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Lemma Lessa (Ph.D.)

ACKNOWLEDGMENTS

First and for most praises and thanks to the Almighty God for the endless blessings and grace that has been a reason for this achievement.

I would like to express my deepest and sincerest gratitude and thanks to my advisor Dr. Lemma Lessa for constructive guidance, wonderful comments, and help with the expertise and precious time throughout this project work.

My special thanks also go to participants of this study at Addis Ababa Health Bureau for their friendly and professional details for the subject matter. I am also grateful to my classmates, Mr. Andualem Aklilu for his unreserved support.

I am extremely grateful to my wife and family for their love, understanding, care, prayers and continuing support to complete my research work.

Antonyo George

June 2020,

Addis Ababa, Ethiopia

Abstract

E-Health systems play an important role in information processing in healthcare for the benefit of the patient as well as health professionals in hospital. Various pieces of literature support that many of e-health applications were developed by using one or more standards in SDLC from start to finish to fulfill the functional requirement and more with a proper set of security mechanisms in place, from the development point of view. However, majority of these security mechanisms were not considered from the users' point of view. As a result, security of health information is becoming an important and growing concern for all those delivering healthcare by protecting sensitive patient records from unauthorized people using security mechanisms.

This research is aimed at answering the following two research questions: How usable are the security mechanisms of e-Health applications in Ethiopia? And how do we improve the usability aspect of the security mechanisms of e-Health applications? The objective is to evaluate usability of security mechanisms of e-Health applications functional at health facilities operational under Addis Ababa Health Bureau and identify strengths and weaknesses of the usability of the security features of the e-Health applications.

This study uses a qualitative research methodology that uses heuristic evaluation of using three e-Health applications by three experts with thematic analysis to identify their focus idea from the collected data. Three e-health systems are widely used by health care facilities in Ethiopia (DHIS2, SmartCare, and OpenEMR). Data collection instrument having thirteen criteria (*Visibility, revocability, clarity, convey features/expressiveness, learnability, aesthetics and minimalist design, errors, satisfaction, user suitability, user language, user assistance, security and privacy)* was adopted from a framework developed by Yeratziotis (2011) dissertation and updated in 2012. The finding reviled that out of the thirteen criteria, *learnability*, *aesthetics and minimalist design*, and *user language* were in compliance, in contrary *revocability* and *user suitability* were not in compliance with security features according to all the experts review of all e-Health applications. Finally, recommendations were given for practice and suggestions forwarded for future research.

.

Keywords: Application Security, Usability, Usable Security, Human-computer Interaction;

Table of Contents

List of Tables

List of Figures

List of Acronyms

AAU	Addis Ababa University
ACL	Access Control List
AHP	Analytic Hierarchy Process
CCTV	Closed-circuit television
CIA	Confidentiality, Integrity, Availability
DHIS2	District Health Information Software 2
EHR	Electronic Health Record
EHRs	Electronic Health Records
EMR	Electronic Medical Record
ePHI	Electronic Protected Health Information
Exp.	Expert
FMoH	Federal Ministry of Health
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
HVAC	Heating, ventilation, and air conditioning
ICT	Information Communication Technology
ID	Identification/Identity/Identifier
INFOSEC	Information Security
IT	Information Technology
IPS	Intrusion prevention systems
ISO	International Organization for Standardization
NCES	National Center for Education Statistics
NGO	None Governmental Organization
RSA	Rivest–Shamir–Adleman (Cryptosystems)
SDLC	System Development Life Cycle
SMS	Short message service

Chapter One

Introduction

This chapter introduces the background of the research, statement of the problem, research questions and objectives, scope of the research, research design, and significance of the study.

1.1 Background

Information Security (IS) has become a major concern of different stakeholders, users, governments, service providers, systems-developers, and systems-administrators (Jang-Jaccard & Nepal, 2014). These concerns are even growing more in health systems. According to the Academy of Engineering and Institute of Medicine (2005), health systems play an important role in information processing in healthcare for the benefit of the patient as well as the hospital health professionals. Additionally, it has many benefits, such as quick and easy access, storage, and retrieval of Patient Health Information (PHI) data in a protected manner for authenticated and authorized users.

E-health application is a health information management system that supports healthcare providers to maintain a record of patients' diagnosis and treatment for current use as well as a future reference (Evans, 2016). Due to the sensitivity of the PHI in these systems, a proper security measure must be in place to protect it from a data breach (Smith, 2019). Many e-Health systems have been developed by the use of one or extra requirements in System Development Life Cycle (SDLC) from start to finish, to meet the purposeful requirement and more with a proper set of protection mechanisms from the development point of view (Bourgeois, 2014). However, these security mechanisms were not considered from the users' point of view (Hof, 2012). In addition, it is a major concern that requires new approaches in systems design to balance the developers' view with the users' view of security mechanism (Dalpiaz, Paja, & Giorgini, 2016). Therefore, e-health applications need to provide effective, high-quality support for providing the best care for patients but without compromising the security.

Protection within the e-health device defines as securing private health-associated information from unauthorized access, use, disclosure, disruption, change, or destruction. Patients worry that

their private medical data may influence their employers' decisions approximately promotions or downsizing or be made public in press reviews or civil court movements (Institute of Medicine, 2009). Also, privacy is the right of persons, agencies, or establishments to regulate private and sensitive information of dissemination for other parties with a proper and indicated use of that information (Holvast, 2009).

Nowadays, many healthcare organizations are vulnerable to security attacks since they contain sensitive patient information (Chowdhury, Jahan, Islam, and Gao, 2018). Patients are required to share information with their physicians to facilitate accurate analysis and treatment, especially to avoid unfavorable drug interactions (Burton, Anderson, & Kues, 2004). Patients trust their health providers if their information is kept private and secure (Institute of Medicine, 2009). This leads them to be more willing to discuss their symptoms, conditions, and past and present risk behaviors. However, patient data can be hacked, manipulated, or destroyed by internal or external users and result in improper modification of diagnosis results that can threaten patient health or even his/her life. Also, patient health information plays a major role in conducting medical research for improving healthcare quality. However, disclosure of health information for various reasons raises concerns about privacy (Institute of Medicine, 1994).

Ensuring the usability of security mechanisms of the e-health system is the key component to maintain the balance of security and usability (Sittig, Belmont, & Singh, 2018). Besides, the e-Health application becomes more secure and usable. But, developing a secure and usable e-Health application is a difficult task due to the higher complexities within the healthcare environment (Ross, Stevenson, Lau, & Murray, 2016).

Usability as per the ISO definition, the quantity to which a product may be used by designated users to acquire exact goals with effectiveness, efficiency, and delight in a specific context of use (ISO-9241/11, 2018). According to Jakob Nielsen (2012), defines usability as a high-quality attribute that relies upon on five additives: learnability, efficiency, memorability, errors, and pleasure. The usability of software program applications is one thing that reduces security and privacy at a significant level (Alshamari, 2016).

If security and usability have been taken into consideration throughout the design of a software program system, it would have helped to reduce the number of security cases, which might be affecting users (Onyimbo and Rad, 2016). The outcome of any software device that implements the balance of each security and usable interface design, might be an outstanding gain, although little has been achieved to deal with those areas (Kainda, Ronald & Flechais, Ivan & Roscoe, 2010). Most of the works that have been accomplished on the balance among usability and security seem to aware extra on the authentication techniques, however it has to move beyond simply this part of a system to think about the mixing into every part of the user interface layout (Nwokedi, Ugochi & Amunga, Beverly & Bashari Rad, Babak, 2016).

Lampson (2009) stated that for usable security to be successful we have to focus on the essential part rather than on the perfection of the systems. Moreover, we need simple models of security that users can understand (Bourgeois, 2014). To make systems truthful we want accountability, and to maintain the freedom we want separate green and red mechanisms that protect the information you care about from the public net (Lampson, 2009).

Security and usability are considered as nonfunctional quality attributes (Mairiza, Zowghi, and Nurmuliani, 2010). Besides, they are not usually considered in the early stages of the development of a software product (Bourgeois, 2014). Rather, their techniques, mechanisms, and best practices are applied as add-ons to user interfaces after the product's development is almost completed (Punchoojit & Hongwarittorrn, 2017).

The safety requirement is considered as top precedence at some stage in the software program development technique in banking and healthcare industries to preserve protection and avoid the dangers or threats. Poor usability can also pose demanding situations within the usage of the systems for which the companies need to recognize the usability improvement technique. Besides, this will help in giving special attention to usability goals, tasks, and workflow of the products, services, and environment (Kulkarni, 2018).

In developing nations, health data from Health Information Systems (HIS) turn out to be a vital factor for strengthening the health structures (Braa, Hanseth, Heywood, Mohammed, & Shaw, 2007). The use of health information is extended not only for patient care and administrative

purpose but also for making plans and decisions for enhancing healthcare delivery (Institute of Medicine, 1994). Therefore, this led to a shift from paper-based to computer-based processing of health information that increase the opportunities for handling patient data efficiently. However, many patient records are lost due to lack of security or there is no well-documented privacy and security policy and procedures implemented in hospitals (Virtual Mentor, 2012). The technological complexity challenge in using the advanced tools of processing health data also raises the security and privacy issues (Abouelmehdi, Beni-Hessane, & Khaloufi, 2018).

Treating employees as a trusted entity, when designing new or improved security processes and mechanisms can significantly benefit the organization and security experts (Vance, 2006). It reduces the organization's exposure to information security risks by improving its security hygiene. Improved efficiency of deployed protection approaches, reduces the overhead impact of protection at the production duties and worker frustration with protection, developing an extra high-quality, participatory approach to maintaining the corporation secured (Kirlappos & Sasse, 2014).

Use of Information Communication Technology (ICT) in healthcare is called e-Health (Kurtinaityte, 2007; Srivastava, Pant, Abraham & Agrawal, 2015). The phrase e-Health is described as an emerging discipline in the coming together of health informatics, society health, and commercial enterprise, relating to health services and information introduced or improved via the internet and ICT (Eysenbach, 2001). Also, in a broader experience, the term characterizes a technical development, but also a state-of-mind, a manner of questioning a mindset, and a dedication for interconnected questioning, to improve health service delivery everywhere using ICT.

Highly sensitive, personal and clinical information recorded and shared in health systems (Institute of Medicine, 1994). An e-Health application, with its security mechanisms in place to protecting this information using proper and usable security mechanisms, becomes very crucial (Sulaiman, Sharma, Ma, & Tran, 2008). Therefore, this study aims to evaluate the usable aspect of security mechanisms that are human interactive and balance security with usability of e-Health applications to address the issue.

1.2 Statement of the Problem

How people interact with security policies and mechanisms is not limited to the point of interaction (Eysenbach, 2001). Usability research suggested that a system with a difficult user interface can harm its functionality, even though a well-designed, easy to use user interface could not have a positive impact if the system does not provide the required functionality (Sasse & Flechais, 2005). In addition, designers dedicate more effort in making a security mechanism as simple as possible, and users still fail to use it simply. The security mechanism which was designed well still needs more effort when they are in use, and users always are drawn to overpass them, especially when users are eager to complete their tasks (Cranor & Garfinkel, 2005). To make an effort for security, users must believe that their assets are under risk and that the security mechanism provides effective protection against that risk (Sasse, & Flechais, 2005).

The deployment of e-Health systems using different platform enables personal health information to be maintained in digital form and ready to be accessed and shared by the right people for the right reason using proper authentication and authorization (Fernández-Alemán, Señor, Lozoya, & Toval, 2013).

The security of health information is an important concern for all those delivering healthcare by protecting these sensitive patient records from unauthorized people using security mechanisms (Institute of Medicine, 2009). These security mechanisms are in place to protect data, systems, and networks (NCES 2003-381, 2003). Also, security experts can handle them to achieve a sufficient level of security for any given system. However, many information systems security mechanisms were not designed based on the consideration of novice users and usability aspects (Hof, 2012). The average end-user often overwhelmed with understanding and using security mechanisms, which are simply annoying end-users (Hof, 2013). In general, security feature of any information system is only as strong as the weakest link on the system, undesirable usability of IT security mechanisms may also result in making errors, resulting in an insecure system (Hof, 2015) which has an impact on the decisions of novice users' usage. Hence, software developers intend to deliver software without a security mechanism than one with difficult or no usability. Security

mechanisms usability is the most undermined attributes of information systems and applications, and also, these attributes were often the afterthought of an afterthought (Hof, 2013).

Security in the systems is found to be one of the barriers in the adoption of ICT in healthcare (Anwar & Shamim, 2011; Kotzé, Paula & Adebesin, Funmi & Greunen, Darelle & Foster, Rosemary, 2013). E-Health application has a security measure to protect PHI from unintended use (Kruse, Smith, Vanderlinden, & Nealand, 2017). Effective security is achieved with the increase of usable security to users and requires the developers to see over the user interface of security tools, where the majority of research and development effort is centered (Sasse, & Flechais, 2005).

Furthermore, the ISO standards with the protection and security of personal information are important to all people, corporations, institutions, and governments. There are special requirements in the health sector that need to be met to protect the confidentiality, integrity, suitability, and availability of personal health information (ISO-27799, 2016). Health information integrity must be protected to ensure patient privacy, and continuity of protection also auditable at all times (ISO 27799, 2008). Effective healthcare delivery is highly dependent on the availability of health information (National Academy of Engineering (US), and the Institute of Medicine, 2005). Health informatics systems security is intended to be operational in the case of disasters, failures, and service denial attacks while protecting the Confidentiality, Integrity and Availability (CIA) of health information, therefore, it requires domain expertise for the health sector (ISO-27799, 2016).

In addition, the act of human error or failure described as an entry of invalid data, accidental deletion, or modification of data by staff to be second categories of security threat (Whitman, & Mattord, 2018). According to Health Insurance Portability and Accountability Act (HIPAA) security rule (2014), indicates the standards that can be applied to protect Electronic Protected Health Information (ePHI), when it is in storage as well as in transit. Also, there are three pillars to address the security protection measure, namely technical, physical, and administrative security in the HIPAA compliance checklist.

The protection of sensitive data is simply as strong as the weakest link, which often turns out to be the human user and not the firewall (Sasse, Brostoff, & Weirich, 2001). This makes the users' consciousness of the data created as well as the threat associated with a data breach is critical,

subsequently shifts from an understanding of complex security procedures to an understanding of organizational pressures. This implies the information security awareness is the key to mitigating security threats caused by human weaknesses (Metalidou et al., 2014). Besides, information security challenges related to employees, face daily must be understood and resolved. Therefore, employees' should have a proper education, and awareness about the significance of information security ought to be a priority of the organization (Margit, 2018).

Usability as a success factor of security, a reliable evaluation of current security mechanisms and procedures in terms of their usability aspect has a great need for application-specific research, which is important (Kainda, Ronald & Flechais, Ivan & Roscoe, 2010). Maintaining security in a digital-technology world has many challenges (Hiranandani, 2011). Risks can be high, varying from loss of information and privacy to loss of important assets (Stoneburner, Goguen, and Feringa, 2002). This demands for advanced security measures to be in place to secure and protect. Moreover, customers or users want the applications to be not only safe but also easy to use. Security measure is deemed to be a trade-off or unbalance between ease-of-use and ultimate security (Yee, 2004; Braz, Seffah, & M'Raihi, 2007). Therefore, this research is aimed to identify the existence of unbalance issues within security and usability, based on the result to recommend a possible improvement solution for the problem.

1.3 Research Questions

1. How usable are the security mechanisms of e-Health applications in Ethiopia?
2. How do we improve the usability aspect of the security mechanisms of e-Health applications?

1.4 Research Objective

1.4.1 General Objective

The general objective of this study is to evaluate the usability of security mechanisms of e-Health applications at health facilities under the administration of Addis Ababa Health Bureau and identify strength and weakness of the usability of the security features of the e-Health applications.

1.4.2 Specific Objectives

In line with the general objective, the research seeks to meet the following specific objectives:

- Identify/formulate evaluation criteria from literature to evaluate usability aspect of security feature in an application
- Analyzing the usability of current e-Health application security mechanisms.
- Propose a possible recommendation to address weaknesses in the current e-Health applications and future e-Health applications.

1.5 Scope of the study

This study covers two main areas, usability, and security. Existing literature and models are used as the foundations of this study on each topic area. Also, integrating the domains of human-computer-interaction and education. This is done to set the context and create a general frame of reference for the rest of the study.

Firstly, background information is given on theories of security, usability, and usability aspects of the security of the e-Health application. Secondly, a set of criteria on the evaluation of the usability aspect of security identified from the literature. Heuristics evaluation of usability was suggested by Jakob Nielsen and Rolf Molich (Nielsen, 1994:29), which are adopted with domain-specific criteria for evaluation undertaken in this study were taken from (Yeratziotis, Pottas, & Greunen, 2012). Thirdly, a heuristic evaluation was conducted by experts, followed by organizing and data analysis using the thematic technique. Finally, in the context of usability of security mechanism issues were identified on the e-Health applications on the study.

1.6 Significance of the study

Evaluating the usability aspect of security on e-Health application is a milestone for the improvement and development of secure and usable e-Health applications. The result of this finding will benefit:

Federal Ministry of Health: the FMoH can use the result of this research to develop or revise the policy and strategy on the e-Health application usability aspect of security mechanisms and this can be used as a guiding tool in the development of e-Health applications.

Developers: the result of this research serves as a guideline for developers to consider the usability aspect of security mechanisms in the e-Health application development.

Health Organizations and Practitioners: the result of this research serves as a starting point for strengthening the security awareness strategy and training about e-Health application for an organizational leader to plan practitioners will adhere to the security policy and procedure.

NGOs and Donors: the result of this research can be used as guidelines to stakeholders to prepare e-Health application security mechanisms to be incorporated in the development phase.

Finally, this study will serve as a springboard for other research on the topic of usability of security mechanisms on other applications.

1.7 Organization of the study

This study constitutes six chapters. The first chapter is the introduction and background of the usability and security topics, research questions, problem statement, objectives, and significance of the study and scope of the study. The second chapter is a literature review that provides both conceptual and contextual ground in the existing knowledge related to security, usability, and evaluation of the usability of security. The third chapter presents the research design and methodology used in this study. The fourth chapter is the analysis, presentation on the collected data. The fifth chapter is discussion on key findings from chapter four. Finally, the last chapter is dedicated to the conclusion, recommendations and future work of this study.

1.8 Summary

The role of e-Health applications in maintaining quality health information is crucial. Having a security mechanism usable to its user is a mandatory element of e-Health system that attributes to the quality of the information and protection against unauthorized access. This research attempts to evaluate the usability of security mechanisms that are in place on three of the commonly

implemented e-Health applications at health care facilities under Addis Ababa Health Bureau and try to suggest improvement on features that are less compline to known standards.

The next chapter deals with the literature review of the research.

Chapter Two

Literature Review

The purpose of this chapter is to review different literature to have a general and core topic area concept about the usability aspect of security mechanisms of information systems in the health domain. Also about the usability issues of security on e-Health applications. Moreover, related work, major models, and theories about the evaluation usability of security mechanisms are reviewed systematically.

2.1 Information Systems Security

Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity. Bourgeois (2016) indicted that information systems security also refers to as follows:

- Access controls, users must have the right authorization to access the system.
- Information protection must be in place by following the information, in-transit, or in-storage.
- Security breaches must be detected at the earliest possible to take remediation within a short time, to minimize the security impact and document the event as well.

2.2 Information Security

Information security, it is important to understand virtually what security is first. In general, security is the state of being secure and free from any danger. In addition, in simple terms, information security is a protection against any adversary or opponent that might harm, with or without intent (National Research Council, 1991). The term indicates information security is the security of information. In a broader expression, information security secures information assets and everything revolves around it (National Research Council, 1991; Whitman and Mattord, 2011).

Information security, ISO defined as the process of securing information. For example, any information in digital or non-digital form only the authorized party with sufficient privileges to view, share or delete (ISO/IEC 27000, 2009*)*.

The security triangle refers as CIA triad shown in (Fig 2.1), a concept of the representations of confidentiality, integrity, and availability at each corner of the equilateral triangle, and at the center of the triangle security, which shows if all of them with equal distance from the central point, then it is said to be balanced and secured. Otherwise, one of the three pillar shifts inwards or outward the balance shift and the equilateral triangle shape also change, then there is a security problem on the unbalanced side of the triangle represents (Perrin, 2008; Whitman and Mattord, 2011).

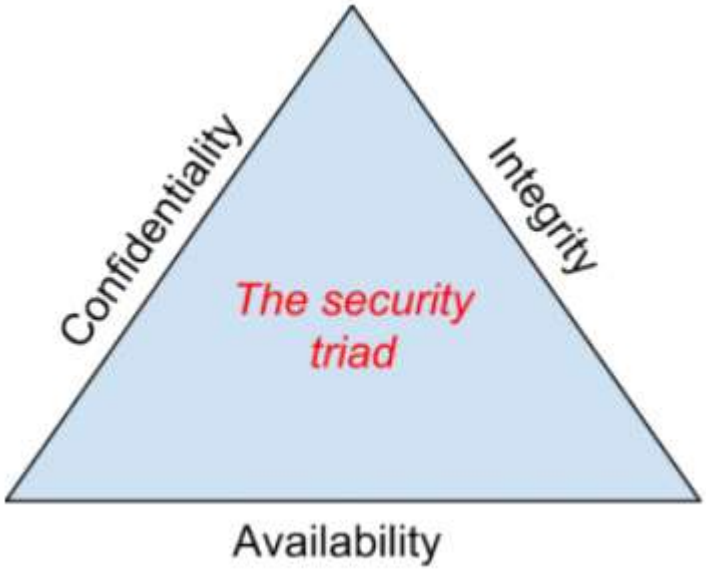


Figure 2. 1 CIA Triad (National Research Council*:* Ch. 6, page 64, 1991)

Discussions to clarify on the CIA triad components according to Perrin (2008), as follows:

- **Confidentiality** - The safeguard of information from unauthorized access, the need for information protection. In another way of saying, privacy as a security concern of confidentiality. For example, only authorized users with access, while unauthorized users denied access to information. File permissions, access control, and encryption of data are used for managing confidentiality on information systems.
- **Integrity** – The protection of information from unauthorized change or modification, information is kept accurate and consistent for authorized access and use. For control

measure, monitor and control authorized access, use, and transmission of information. For example, user account controls should not be modifiable, leads to service interruption and confidentiality breach. In the case of user files modification, it leads to data loss but reversible if version control systems and backups were kept, which are the most common measures used to ensure integrity.

- **Availability** - The protection of information should be available, for the right user, at the right time, at the right place, when the information is needed. Security measures for ensuring the information is available at all times, each of the system components such as data system, access channels, and authentication mechanisms must be protected. Besides, high availability systems are designed toward improving availability.

2.3 Security Mechanisms

In this section security mechanisms, authentication, and access control are discussed based on the literature review of other works, concerning the research question.

2.3.1 Authentication

Identification is a process of verification, a user's identity checked against user's information already existed in the system user's database. Authentication is a process of tying an identification, identifier (ID) to a designated entity. These identifiers (IDs), specific IDs with authorized users of IDs in a computer system should be related. For example, passwords are widely used for the user authentication method by using a combination of a user (ID) and password for a specific user, with serious vulnerabilities (Sandhu, Hadley, Lovaas, & Takacs, 2015). Other authentication methods are available besides user password, such as a key or card, biometrics, multi-factor authentications, Rivest–Shamir–Adleman (RSA-Cryptosystem), SecurID token which generates a new access code every sixty seconds (Bourgeois, 2016).

All views relating to private access, i.e. access control to data and assets saved in storage are subjected to verification (Kiennert, Bouzefrane, & Thoniel, 2015).

2.3.2 Access control

Access control frameworks, which merge security, character administration, and trust models with a clear way for the establishments of programming frameworks of security. Hence, with the investigation of character administration, trust models, and the hypothesis on the access control models (Benantar and Messaoud, 2006).

Controlling access to assets is one of the central topics of security. Access control addresses more than fair, which users can get to which records or administrations. It is approximately the connections between substances (that's, subjects and objects). Access control constrains what a person can do on demand, as well as what application executions on behalf of the users are allowed to do. On this manner access control seeks to protect that might lead to a breach of security (Sandhu & Samarati, 1994).

The objective of access control is to minimize the chance of unauthorized access to physical and logical systems. Access control may be an essential component of security compliance programs that guarantees security innovation and access control approaches that are input to secure secret data, such as client information (Bourgeois, 2016). Also for each data asset that an organization wishes to oversee, a list of clients who can require particular actions can be made. Usually, an access control list, or ACL. For each client, particular capabilities are allotted, such as read, compose, erase, or include. As it were clients with those capabilities are permitted to perform those capacities. In case a client is not on the list, they cannot indeed know that the data asset exists (Bourgeois, 2016).

2.4 Usability

The official ISO 9241-11, the most widely adopted definition of usability is the magnitude to which a product can be used by distinctive users to acquire detailed goals with effectiveness, efficiency, and satisfaction in a designated context of use. Also, Nielsen (2012), in which he explained usability as the quality attribute of a system that examines how easy it is to use the system. He also further defined usability in terms of five key quality components as listed below:

- **Learnability**: How easy is it for users to accomplish basic tasks the first time they encounter the design?
- **Efficiency**: Once users have learned the design, how quickly can they perform tasks?
- **Memorability**: When users return to the design after a period of not using it, how easily can they restore proficiency?
- **Errors**: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?
- **Satisfaction**: How pleasant is it to use the design?

Information system usability incorporates strategies of measuring convenience, such as needs examination and the anticipation of the standards behind an object's seen effectiveness or tastefulness (Bergaus & Behringer, 2015). In human-computer-interaction and computer science, usability considers the class and clarity with which the interaction with a computer program or web usability is designed (Valverde, 2011).

2.5 Usable Security

Usable security is a field that explores the complexities that client's involvement when they interact with security features (Garfinkel & Lipford, 2014). Most applications now have security highlights or introduction that associated with clients. In any case, due to their need for convenience, clients frequently dodge and indeed disregard their security responsibilities (Kainda, Fléchais, & Roscoe, 2010).

The interaction between the human element and the technology, design of the interface, has a problem. This problem relates to the research discipline of human-computer interaction as much as it does to the discipline of information security. Creating usable security has ended up a need and is well supported (Furnell et al., 2006; Whitten and Tygar, 2005)

When looking to secure data assets, organizations must adjust the requirements for security with users' to successfully access and use. In case a system's security measures, which makes it impossible to utilize, at that point clients or users tend to find other means to avoid security, which makes the security mechanisms more helpless than it would have been without the security

measures. For example, in the case of secret passwords, organizations require a greatly long catchphrase with a few extraordinary characters, a representative may give an option to write it down and putting it in a drawer since it will be incomprehensible to memorize (Bourgeois, 2014).

2.6 Evaluating Usability

The survey of five universal benchmarks shows concerned with characterizing and assessing ease-of-use of data innovation and intuitively frameworks. The point is to inspect the level to which the universal guidelines give rules for arranging and conducting ease-of-use assessment of data frameworks. They begin by comparing the benchmarks in arrange to reveal the contrasts and connections between the rules given. At that point, based on the rules, we offer a system that highlights the exercises required for ease-of-use assessment of data frameworks (Marghescu, 2008).

A study on usability evaluation by Riihiaho, (2001) shows encounters in usability, gathered from 72 assessments between the periods from 1993 to 1999. In the assessments, both program and implanted frameworks have been considered, usability assessment is a basic step in a human-centered plan, an assortment of convenience assessment strategies is required in preparation of an improvement, since ease-of-use may be a complex multidimensional concept that ought to be looked at in numerous ways. Distinctive strategies serve diverse assessment purposes and uncover distinctive issues. In this manner, a few strategies ought to be utilized as a complement to each other. In this proposition, usability assessment strategies are isolated into experimental client testing and ease-of-use assessments without client involvement. The foremost common client testing strategy may be the ease-of-use test in which a member give activities with the assessed framework. Also, the common ease-of-use review strategy could be a heuristic assessment in which an examiner assesses a client interface with a set of convenience rules.

A brief discussion on usability evaluation methods:

- **Heuristic evaluation** - is a casual framework review strategy where few evaluators are displayed with an interface plan and inquired to judge whether each of its components takes after a set of setting up the ease-of-use standards (Nielsen and Molich, 1990). Heuristic

assessment can be done by specialists and non-experts. It is troublesome to do a heuristic assessment with a single evaluator; it is close inconceivable for one individual to discover all convenience issues. However, it has appeared that when there are numerous evaluators, each was able to discover distinctive ease-of-use issues, hence the viability of the issue can be made progresses by having a gathering of evaluators. Ordinarily, 3 or 5 evaluators can report close to 70% of ease-of-use issues; extra evaluators frequently are not able to discover much more extra issues (Nielsen and Molich, 1990).

- **Cognitive walkthrough** - could be a hypothetically organized convenience assessment handle that focusses on a user's cognitive exercises, particularly whereas performing an activity. It can be carried out by individual or groups of people, computer program engineers or usability pros, and on wrapped up items or paper models. Based on a hypothesis of exploratory learning and corresponding interface plan rules, a cognitive walkthrough may be a task-based strategy that centers an evaluator's consideration on the user's objectives and activities within an assignment, and on whether the system design underpins or prevents the achievement of those objectives. Additionally, it may be a form-based assessment technique in which depends on a set of shapes to direct the assessment handle (Rieman, Franzke, and Redmiles, 1995).
- **Scenario-based** - is the representation of individuals utilizing innovation and it is basic in examining and analyzing how the innovation is utilized to reshape their exercises. A situation portrays a grouping of occasions when collaboration with a framework from the users' viewpoint and a framework is built from indications of the situation and its impacts can be felt. 'Scenarios' are comparative to 'Use Cases', which indicate that a modern view-at-convenience test strategies of interfacing for human-computer interaction intuitive at a specialized level. But scenarios can be effectively caught on by anybody in any case of the level of their specialized information (Rosson, John, and Carroll, 2002).
- **Remote Testing** - Members that were selected are welcomed to come to the test offices comprising of a test room, where the members will fulfill particular assignments, a perception room, and the "recording" room. Ease of use research facility may contain complex and advanced audio/visual recordings and examination offices. In this setting, test sessions are conducted exclusively. Inaccessible ease-of-use assessment indicates to a

circumstance in which the evaluators and the test members are not within the same room or area. The users' behaviors are captured, add up to, and visualized to appear the net pages individuals investigated. The visualization appears the foremost common ways taken through the site for a given assignment, as well as the ideal way for that assignment as executed by the architect (Atterer, Wnuk and Schmidt, 2006).

- **User-based Testing** - usability evaluation strategies in which clients straightforwardly take an interest. Clients are welcomed to do routine tasks with an item or inquired to investigate it unreservedly, whereas their behaviors are watched and recorded in arrange to recognize plan faults that cause client errors or challenges. Among these perceptions, the time required to total task, assignment completion rates, and number and sorts of mistakes, are recorded. Client testing is centered on the input of clients associated with a specific interface and is ordinarily conducted in a scenario-based environment. Client testing is sweet at surveying the framework inactivity, at distinguishing issues clients encounter whereas performing genuine tasks (Smith, 2010).
- **Focus group** - A center gather could be an assembly of almost six to nine clients wherein clients talk about issues relating to the framework. The evaluator plays the part of the arbiter and gathers the needed data from the talk. This is often profitable for moving forward the convenience of future discharges. This strategy could be a method utilized to consider human-computer interaction and human variables (Rosenbaum, Cockton, Coyne, Muller, and Rauch, 2002).
- **Contextual inquiry** - It could be a field investigate strategy wherein ease-of-use evaluators go to the users' work environments, watches them at work, and inquires questions concerning the work substance, prepare, or item utilization. A few evaluators may watch diverse clients at the same time. The information is assembled, compared, and shared among item development team members after the perception. It may be an organized field meeting strategy, relevant request is based on three center standards: 1) understanding the setting in which a product is used is basic for an attractive plan, 2) that the client is an accomplice within the plan handle, 3) that the convenience plan forms, counting evaluation strategies like relevant request and ease-of-use testing, must have a focus (Raven and Flanders, 1996).

The ease-of-use plan of the human-computer interface decides the advertising prospect of the product. Designers ought to be guided by the normal and human thought too, architects ought to optimize the utilization and operation of the interface from numerous diverse zones, such as plan, ergonomics, cognitive brain research, phonetics, and semiotic, eventually accomplish the perfect objective of progressing the convenience of items. Convenience assessment is possessing a central portion of program advancement based on the outcome about extracted from quantitative and subjective assessments. Concurring to investigate none of these strategies is predominant over others (Ghasemifard, Shamsi, Kenar & Ahmadi, 2015).

2.7 Heuristic Evaluation Guidelines

Even though numerous groups of researchers have created heuristics, one of the known sources is the set created by Nielsen's (1994). Nielsen refined the list initially created in 1990 by himself and Rolf Molich. Nielsen's Heuristics incorporate:

- **Visibility of system status**: The framework ought to continuously keep clients educated around what is going on, through fitting criticism inside sensible time.
- **Match between system and the real world**: The framework ought to talk the users' dialect, with words, expressions, and ideas familiar to the client, instead of system-oriented terms. Take after real-world traditions, making data show up in a common and consistent arrangement.
- **User control and freedom**: users regularly pick features through mistake and will need a clearly marked "emergency exit" to leave the undesirable state while not having to undergo an extended dialogue. Support undo and redo.
- **Consistency and standards**: users should no longer need to wonder whether different words, situations, or moves imply the same.
- **Error prevention**: it is obvious that a well-designed error messages could prevent an error from happening in the first place. A good practice would be avoiding conditions that could possibly lead to an error but if it is not the case, proper notification should be displayed for users before they commit to the action.

- **Recognition rather than recall**: reduce user's memory-load by making objects, actions, and options visible. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
- **Flexibility and efficiency of use**: alternate methods for accomplishing a frequent action (such as hot keys) may often speed up the interaction for the expert user such that the system can provide to both inexperienced and experienced users.
- **Aesthetic and minimalist design**: messages should not contain information which is unnecessary or rarely needed. Extra information reduces visibility of the relevant once.
- **Help users recognize, diagnose, and recover from errors**: error-messages should be expressed in an easy-to-use language, indicate the exact problem, and suggest a solution constructively.
- **Help and documentation**: it is better if any user can use a system without documentation, but it might be necessary to provide help-text and guide. These documentations should be easily searchable, user's task centered, with all steps likely to be carried out by users, and with manageable size.

2.8 Expert Heuristic Evaluations

Users or specialists can do heuristic evaluation. In the evaluation, the evaluators use well-known heuristics principles. In addition, a heuristic evaluation is done using usability experts to review the applications or sites' interface and compare it with the accepted usability principles or guidelines. The examination outcome will identify potential usability problems (Nelison, 1994).

2.9 Framework for Evaluation of Usable Security

A framework developed by Yeratziotis (2011), a three-phase process to develop a level of security heuristics checklist for evaluation of usable security. The usable security heuristic assessment is the third component of the system to assess usable security in online social systems and is presented in fig 2.2 below.

Yeratziotis (2011), the framework illustrates that the design of security and privacy features for website or application should be usable, with the consideration of security is an area that most

users avoid due to the reason of its complexity. To make this complexity to be user-friendly without compromising the security, evaluation of the usability of security feature using the suitable and domain-specific method was needed for identification and improvement. Furthermore, heuristic evaluations are a popular usability inspection method that enables Human Computer Interaction (HCI), experts to evaluate the usability of interfaces of applications, and web sites. Finally, he suggested that a systematic process is required to develop a set of usable security heuristics, namely a three-phase process constructed for the development of the usable security heuristics for specific application domains. The three-phase process is shown in detail in fig 2.2 below.

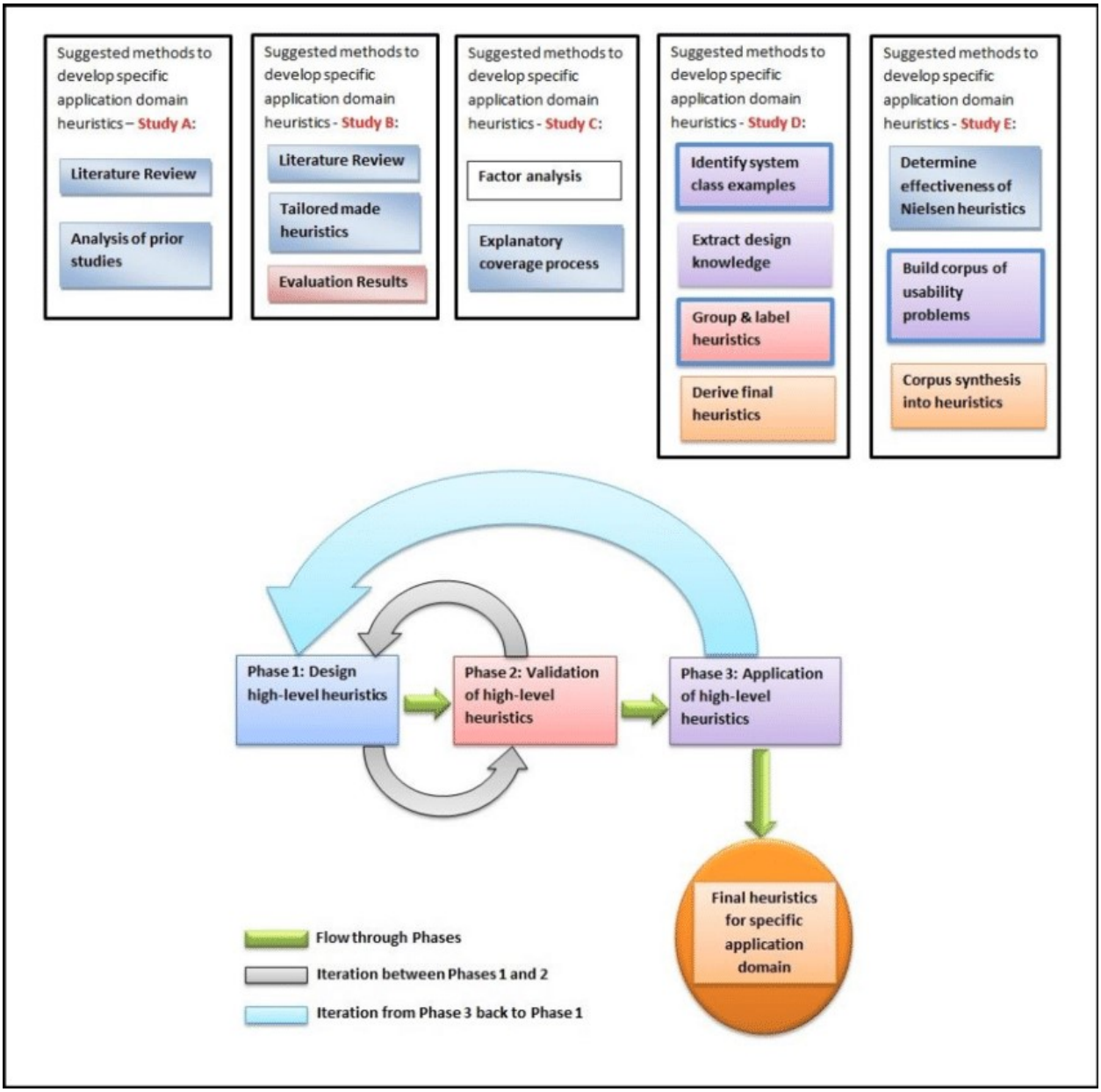


Figure 2. 2 Three-phase processes for developing security heuristic (Yeratziotis, 2011).

The following list shows criteria of security heuristics adopted from (Yeratziotis, Pottas, and Greunen, 2012) in brief:

1. **Visibility -** the system should keep users informed about their security status.
2. **Revocability -** the system should allow users to revoke any of their security actions.

3. **Clarity** - the system should inform users in advance about the consequences of any security actions.
4. **Convey Features⁄Expressiveness -** the system should guide users on security in a manner that still gives them freedom of expression.
5. **Learnability** - the system should ensure that security actions are easy to learn and remember.
6. **Aesthetics and Minimalist Design** - the system should offer users relevant information relating to their security actions.
7. **Errors** - the system should provide users detailed security error messages that they can understand and act up on.
8. **Satisfaction** - the system should ensure that users have a good experience when using security and that they are in control.
9. **User Suitability -** the system should provide options for users with diverse levels of skill and experience in security.
10. **User Language -** the system should use plain language that users can understand with regard to security.
11. **User Assistance -** the system should make security help apparent for users.
12. **Identity Signal -** the system should have valid certificates and the information should be available on the browser of use.
13. **Security and Privacy** - the system needs to consider integrity, availability, confidentiality, and privacy.

A heuristic assessment is considered as an expository assessment strategy that is embraced by usability specialists. They apply a specific guideline of heuristics to assess the usability of a user interface. This gives a prompt investigation of the website/application, which makes a difference to correct confusing components within the current plan and leads to improved client encounters. The strategy is widely used because it is symptomatic and point-of-view examination for recognizing issues from user in a brief time. Particularly, its' reason is to recognize issues that are related to the plan of client interfacing. The outcome is reliant on the experts' broader experience with ease of use (Nielsen, 2005a; Straub, 2003).

A few specialists working autonomously were considered satisfactory and exceptionally successful in recognizing usability issues. Nielsen (2005b), reached to the conclusion that between three to five evaluators are adequate, as they would be able to find up to 75% of usability issues on the user interface, fig 2.3 shows in detail.

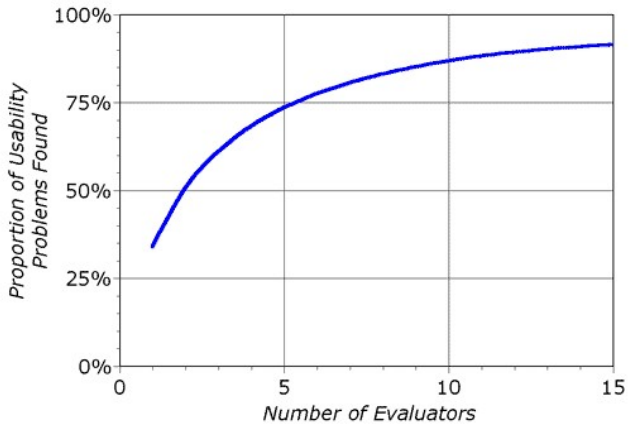


Figure 2. 3 Number of experts for usability evaluation, by Jakob Nielsen (1994)

2.10 E-Health Applications

By 1992, hardware had turn out to be extra affordable, powerful, and compact, and the use of Personal Computer (PC), Local Area Networks (LANs), and the internet gave access to quicker and simpler to get access to medical information. Electronic Health Records (EHRs) were firstly developed and used at educational medical facilities however, because most have been replaced by EHRs from suppliers. While EHR use has wide spreads and clinicians are being prepared to practice in an EHR-mediated world, technical issues have been overshadowed with the help of procedural, professional, social, political, and in particular ethical issues as well as the need for compliance with requirements and information security. There have been massive progressions that took place, but most of the early desires of EHRs has not been realized and current EHRs still do not meet the need of today's dynamic healthcare environment (Evans, 2016).

The foremost broadly utilized e-Health applications are Electronic Medical Record (EMR), which may be an advanced form of a patient's therapeutic history from a specific health facility. In any case, numerous organizations are utilizing applications that permit a patient's record (EHRs) to be

accessible by numerous health facilities (Ajami & Bagheri-Tadi, 2013). EHRs allow for better quality and continuity of healthcare services, because health care providers; specialists; hospitals; and nursing homes share records easily. Information sharing is therefore not limited to geographic regions (Burton, Anderson, & Kues, 2004).

E-Health is a developing field that merges medical informatics, public health, and business referring to health services, and information delivered or enhanced using the internet and ICT (Eysenbach, 2001). In a wider sense, e-Health is characterized as, not only a technical development but also a state-of-mind, a way of thinking, and an attitude to improve health care services everywhere by using ICT (Eysenbach, 2001).

2.10.1 The Security-Related Challenge of e-Health Applications

The challenge of e-Health systems in regards to security and privacy issues such as unauthorized access to patient's digital records, attack on personal health records, cybersecurity issues (Idoga, Agoyi, Coker-Farrell, & Ekeoma, 2016). These challenges have an impact on the e-Health applications in providing trustworthy and reliable data to the e-Health system, users and health care providers, as an attack on the e-Health applications can threaten the smooth operations of the system (Idoga, Agoyi, Coker-Farrell, & Ekeoma, 2016).

2.10.2 Security Mechanisms of e-Health Application

The Health Insurance Portability and Accountability Act (HIPAA) includes five complex regulations. These regulations address protection of the security/privacy of medical records. Currently the HIPAA have incorporated rules that address implementation of electronic medical records that defines how health information is protected. The rule sets standards for the use, disclosure and what needs to be followed while working with health data in order to protect patients' private medical information. The HIPAA also complements the implementation of physical, technical, and administrative safety measure to assure the protestation of PHI privacy (Moore & Frye, 2019).

Moore and Frye (2019), further described the HIPPA safety measures as:

Physical Safety Measures - refers to the physical access to PHI. This may include access to a location or physical object like buildings, offices, secured areas, computer hardware, and files. **Technical Safety Measures -** refers to access control to computer systems and the protection of electronic transmission of PHI. Technical security addresses who and how a person may access, view and use electronic medical records. PHI must be encrypted while it is being transmitted between locations. Facilities are required to implement procedures, software, and equipment to protect PHI including encryption and decryption in backing up and restoring operations. **Administrative Safety Measures -** require facilities to create and update policies and procedures for employees to learn and follow to help ensure the security of PHI. Some examples are: acceptable use policies, sanction policies, information access policies, security awareness training, and contingency planning.

2.11 Related works

Several researches have been done by scholars from abroad regarding usable security issues using standards and guidelines. Some of them are presented as follows:

A study conducted by Yeratziotis, Greunen, & Pottas (2011), on evaluation of two online health social networks that provide health information and health services that permits patients to share their PHI with other patients and their health-care providers. Based on the result the researchers recommended on the improvement of the two online health social network usability features focusing on the criteria, trust, ease-of-use, terminology, ease-of-learning, feedback, awareness, errors, and help & documentation. In addition, in their study they have also concluded that improvements on the criteria may have positive influence on their adoption by the intended users.

In their research article conducted in 2012, they revealed the continuous and increasing popularity of providing health services over the Internet. These services were turning into more complex and being designed in the context of social networking paradigms. The reality that their usefulness and success had been dependent on user willingness to share and publish their PHI not be underestimated. This, in turn, leave the users with legitimate concerns regarding the security and

privacy of the applications, despite their benefits. Heuristic evaluation on usable security, which was conducted by Yeratziotis, Greunen, & Pottas (2012), was a component of a larger research project, which aimed to provide a process for developing heuristics evaluations method that can be applied in security and privacy. In their research article, they highlighted the need to design applications with security and privacy that is usable for their respective users, hence, the emergence of field of study in usable security. These are required to assist software developers in their designs. Their belief was that usable security can have a pivotal and positive influence on the adoption and usage of services in online health social networking environments.

Another research on related topic was conducted by Alenezi, Kumar, Agrawal, & Khan in 2019. Their research focused on usable-security attribute evaluation using Fuzzy Analytic Hierarchy Process (Fuzzy-AHP) using the following attributes: satisfaction, efficiency, effectiveness, availability, confidentiality, and integrity.

They pointed out that high secure software has less usability and has poor businesses continuity. Besides using the services of software, high security turns out to be worthless. Hence, there was a need to bridge the gap between security and usability of software. In their research they tried to identify the main factors of security and usability that affect each other directly and indirectly, including confidentiality, integrity and availability and effectiveness, efficiency, and satisfaction. To evaluate their work they used the Fuzzy Analytic Hierarchy Process (Fuzzy AHP). They obtained results and conclusions were assumed useful to software developers to achieve more secure and usable software.

Based on an initial argument that, in respective of having online banking at the convenience of users, there are people who were skeptical in its utilization due to awareness and security concerns, Mahmadi, Zaaba, & Osman (2016) performed a survey that highlighted the subject of, online banking security in Malaysia, from the perspective of the end-users. Their study was done by assessing HCI, usability and security. The online survey they conducted utilized 137 participants to have initial insights on security challenges of online banking in Malaysia. As a continuation of the results, interview was conducted for 37 participants to dig deeper for clear understanding about end-users perception on online banking within the context of usable security.

The outcome indicated that majority of the end-users were frequently challenged especially with technical jargons, security features and other technical issues. Even though the security features were placed to ensure protection, users were incapable to go in line with the technical aspects of such features.

2.12 Summary

In this chapter, relevant literature were reviewed on these topic areas such as security, usability, usable security, evaluation of usability, and heuristic evaluation method. Usable security topic area with the evaluation process, strategies, techniques, are identified to help conceptualize, the evaluation process. Also, the security heuristic framework is identified as an evaluation method of usable security. Moreover, the expert heuristic evaluation method reviewed. The next chapter deals with the methodology and design of the research.

Chapter Three
Research Design and Methodology

This chapter presents the research design and techniques in detail used in this study respectively to address the research objective. To accomplish this, a researcher starts to search for a related topic area from literature, in respect to the research objective. This helps to pave the way how to reach the result with a focused lens of appropriate methodology, and data analysis (Jagadeesh, Balakumar, & Inamdar, 2013).

3.1 Research Design

A research design is a conceptual blueprint within which research is conducted, the researcher formulates an action plan as a to-do list to incorporate the steps and means of collection, measurement, and analysis of raw data (Akhtar, 2016).

Qualitative research design is the most flexible of the other research techniques with a variety of accepted methods and structures, used for experts' comments and opinions (Astalin, 2013). The research methodology comprises of research methods that can be used for collecting, analyzing, and interpreting the data, for sufficiently answering the research questions (Goundar, 2012). The suitable research methodology highly based on the nature of the research and its objective. The qualitative method is used for this study with descriptive, which tries to address the research objective.

The research design in this study follow these steps of processes:

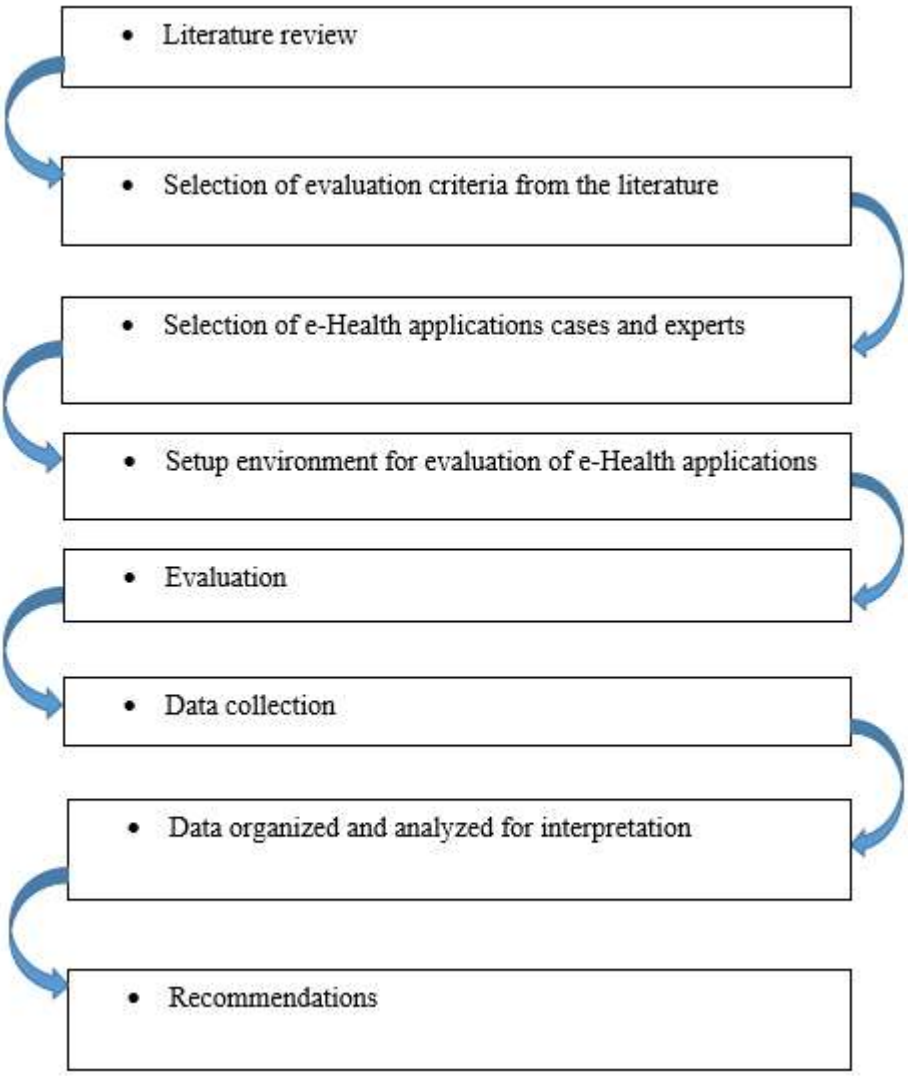


Figure 3.1 Research design

3.1.1 Research Approach

Qualitative research attempts to communicate an event of a particular group's experience in their own words with a narrative. Which is indicated with a transformative worldview, narrative design, and open-ended interviewing (Creswell, 2013). Researchers more accustomed to the traditional deductive approach and qualitative research logic can be challenging for researchers, which

employs an inductive approach. The researcher first collects data and then attempts to derive explanations from those data. Also, qualitative research tends to be more exploratory, aims to provide insight into the research problem (Suter, 2012). Qualitative research can produce large amounts of data, which include a word for word notes or transcribed recordings of interviews or focus groups, jotted notes, and more detailed "field notes" of observational research, a diary or chronological account, and the researcher's reflective notes made during the research. These data only provide a descriptive record of the research without explanations. The interpretation makes sense for these data to further explain the phenomenon (Pope, 2000). Qualitative research allows the researcher to gain access to the research participants' thoughts and feelings, which enables them to understand the meaning of their experiences (Sutton & Austin, 2015). Therefore this research follows a qualitative research method to address the research objective.

3.1.2 Research Strategy

The research strategy demonstrates step by step actions and process on how to answer the research question by the researcher. Different types of research strategies are available; ethnography, survey, experiment, grounded theory, narrative, and case study, selection of one highly depends on the research question (Creswell, 2013). The current study has adopted a case study with a checklist instrument as a strategy.

3.1.3 Study Setting

The e-Health applications OpenEMR, DHIS2, and SmartCare are installed on laptop or desktop and configured without any clinical data, to protect data privacy, even though the evaluation were done only on the security mechanisms. On the other hand, DHIS2 has an online demo version is available for the evaluation. After all the necessary setup and configuration ready, meeting with the experts for introduction about the overall evaluation process and research objective to have a clear awareness between the experts.

3.1.4 Case Selection

The case selection is the determination of the balanced phenomenon of at least one case as the specific subject of research. The purposes behind choosing a case or cases shift from enthusiasm

for the specific case to hypothetical contemplations (Mills, Durepos, & Wiebe, 2010). Purposeful sampling is used for the selected cases of e-Health applications for evaluation. Addis Ababa Health Bureau also communicated for the first level of information regarding e-Health applications that are found and in use in the public facilities, currently, SmartCare and DHIS2 are being used in public facilities throughout Ethiopia. For the case of OpenEMR as an open-source application, NGOs tend to support it with a customized way for the number of health facilities. This study focused on the security mechanisms of the E-health applications, for the evaluation of the usability aspect for the intended users of these applications.

3.1.5 Study Participants

A member of the expert group of the study is selected purposively. These experts must have a relevant knowledge and experience of the health domain and e-Health application are the major criteria used in selecting experts. In fact, their willingness to participate in the study counts by far more. The major attribute of the expert group is displayed in the table (table 3.1) below.

Table 3. 1 Experts profile information

Experts	Exp.1	Exp.2	Exp.3	Exp.4	Exp.5
Consent is given for participation (Y/N)	Yes	Yes	Yes	Yes	Yes
Age	38	38	35	41	33
Sex	Male	Male	Male	Male	Male
Highest Education Level	B.Sc. Engineering Degree	M.Sc.	M.Sc. in Information Science	M.Sc. In Information System and Technology	B.Sc. in computer science and Masters in Social work
Years of work experience	15	12	14	20	10
Domain of Work	Networking, Health Informatics, System Admin	E-Health	Management Information System Manager	E-Health	MIS (Management Information System)
Evaluation of Start date	Mar 5, 2020	Mar 5, 2020	Mar 5, 2020	Mar 5, 2020	Mar 5, 2020
Evaluation submission date	Mar 26, 2020	Mar 24, 2020	Mar 29, 2020	No Submission	No Submission

3.2 Research Technique

In this study security heuristics, checklist and focus-group-discussion are used to conduct the research. The security heuristics checklist is composed of yes and no answer with the experts comment on each criterion. The first step of evaluation on each application is evaluated with all the experts. In this study, the security heuristics checklist is adapted from a framework "*A Framework for Evaluating Usable Security: The Case of Online Health Social Networks*" to conduct the evaluation (Yeratziotis, Pottas, & Greunen, 2012).

3.2.1 Data Collection

Qualitative studies highly founded on non-random sampling methods and the use of non-quantifiable data such as words, feelings, emotions (Kabir, 2016). For the collection of these types

of data, different methods are available among them open-ended questions with checklist instrument is used in this study.

Open-ended questions and inquiry of in-depth responses about people's experiences, perceptions, opinions, feelings, and knowledge. Data consists of verbatim quotations and sufficient content/context to be interpretable (Patton, 2002).

A security heuristic checklist was used as a data collection instrument in this study. The checklist has thirteen criteria, which also have further sub-criteria.

3.2.2 Data Analysis Strategy

Qualitative research mainly collects unstructured text-based data, which is in the form of interview transcripts, observation notes, and diary entries. In some cases, qualitative data can also include a pictorial display, audio or video clips, or other multimedia materials. Data analysis of qualitative research is more of a dynamic, intuitive, and creative process of inductive reasoning, thinking, and theorizing (Basit, 2003).

Thematic analysis, which is a common data analysis strategy for qualitative data, that is concerned with the identification and analysis of patterns of meaning themes and constitutes a widely applicable, cost-effective, and flexible tool for exploratory research. Thematic analysis is particularly suitable for analysing experiences, perceptions, and understandings. It is appropriate for the analysis of small, medium-sized, and even large data sets (Clarke, and Braun, 2013).

According to Braun and Clarke (2006) indicated the six phases of thematic analysis processes this study adopted as a strategy for data analysis indicated in brief as follows:

- **Familiarisation with the data**: for a clear understanding of data by repetitive reading and listening to recorded media data and noting any initial analytic observations.
- **Coding**: the researcher codes every data item through the analytical process to capture a semantic and conceptual reading of the data, to extract relevant data.
- **Searching for themes**: if codes are the bricks and tiles in a brick and tile house, then themes are the walls and roof panels. Searching for themes is a bit like coding your codes to identify similarity in the data, to extract the relevant theme.

- **Reviewing themes**: involves checking that the themes work for both the coded extracts and the full data set. The researcher should reflect on whether the themes tell a convincing and compelling story about the data and begin to define the nature of each theme and the relationship between the themes.
- **Defining and naming themes**: to conduct and write a detailed analysis of each theme (the researcher should ask 'what story does this theme tell?' and 'how does this theme fit into the overall story about the data?'), identifying the 'essence' of each theme and constructing a concise, punchy, and informative name for each theme.
- **Writing up**: an integral element of the analytic process, which involves weaving together the analytic narrative and data extracts to tell the reader a coherent and persuasive story about the data, and contextualizing it with existing literature.

3.2.3 Validity and Reliability

The accuracy and truthfulness of scientific research must be valid and reliable. The examination of collected data, to what extent it covers the actual research, referred to as validity (Ghauri, & Gronhaug, 2005). Validity means "measure what is intended to be measured" (Field, 2005).

Reliability is the measurement of scientific research to what extent it provides stable and consistent results (Carmines, & Zeller, 1979). Reliability is also concerned with repeatability, which indicated by Moser and Kalton (1989) a scale or test is said to be reliable if repeat measurement made by it under constant conditions will give the same result.

The validity and reliability of this study, which is qualitative research, data collected from participants must confirm with the consent for the data validation, through e-mail communication.

3.3 Summary

The research methodology is discussed in this chapter. Also, the procedures, on how to address the research objective has been discussed in this chapter. Finally, the data analysis process of this research is presented. The next chapter will discuss the data presentation, analysis, and discussion of this research.

The chapter outline in two parts to describe the overall research design and method of the thesis. The first part of the research design is on the selection of a research method, which is a qualitative research method with a case study approach. The study setting and sampling method, which is a purposeful sampling method for the applications as well as the participants' in brief. In the second part, the research technique is discussed with the data collection method is used, open-ended questions and focus-group-discussion chosen. Also for data analysis strategy, the thematic method is used on data to present and discuss. Finally, the validity and reliability of the study discussed.

Chapter Four

Data Analysis and Presentation

This chapter presents the results of the study after analyzing the collected data from experts with heuristic evaluation methods. The results were extracted from the security heuristic checklist, with three experts participated.

4.1 Data Organization and Participant

The study participant for this study was five experts out of which three participants finished the evaluation of three e-Health applications using security heuristics. The researcher also uses a phone call for communication means for clarification on the checklist as well as to create a clear and common understanding of the objective of this study among the experts.

Each application with three experts filled evaluation checklist data entered in Microsoft excel sheet to organize and make it the analysis step easy and visible. The thematic method was used for data analysis on each application expert's comment to examine the focuses or patterns of meaning within data of each sub-criteria on the security heuristic checklist output shown (Appendix E). Furthermore, (Appendix F) illustrate expertise agreement on each subcategory of security heuristic checklist. Finally, this commonality and differences in each application for each security heuristic checklist response were cumulated to get the overall result of the evaluation.

4.2 Analysis and Presentation-Part-1

In this section the first part of data analysis of thirteen criteria's or principles is presented based on the thematic output of (Appendix E) of three experts' evaluation in detail as follows:

4.2.1 Visibility

To understand the visibility of the e-Health systems that are selected for the study, one needs to investigate how the selected applications should keep users informed about their security status (Nielsen, 1994). Accordingly, from the review of experts, there were no noticeable delays in the OpenEMR, DHIS2, and SmartCare applications from their response time perspective in response to a security-related action. As a result, the users are not kept informed or notified regarding delays

in the three systems. If there is an error in typing the security parameter, all three application's pop-up windows do not display security-related error messages with the field-specific to the error.

After a user completes a security action, only OpenEMR provides feedback that indicates the next group of actions that might be started. On the other hand, DHIS2 and SmartCare don't have such a feedback feature that indicates what to do next after a successful login. There is some form of feedback such as a welcoming window or another workspace window for every security-related action in all the three eHealth applications.

4.2.2 Revocability

The revocability of the e-Health system examines how the system allows users to revoke any of their security actions (Yee, 2002). De-selection of checkbox and group selection of security options in menus were possible for OpenEMR & SmartCare applications but it was without a visible notification, whereas in DHIS2, application errors were highlighted in red and request users to correct their entry. Reversing security action is not an easy task for the applications because all do not have the means to undo or revert any security action. Prompts of security actions or words used in the messages clearly and consistently describe the respective actions for all three applications. Also, the applications are designed in a way that keys with similar names perform similar actions.

Users are not allowed to terminate a security action that is on progress right in the middle of the process in all three applications. No instance for termination action in progress in DHIS2, even though SmartCare does have a close button that cannot stop the progress of only a short time to execute the security action. All applications, do not have an 'undo' function at the level of a single security action or for a complete group of security actions.

4.2.3 Clarity

The clarity criteria help to investigate how the e-health systems inform in advance about the consequences of any security actions (Yee, 2002). The user roles defined in the system happens to notify users with possible drastic and destructive consequences that might result from their security actions in all three applications and prompt users to summarize the change on sensitive data. Unlike

DHIS2, OpenEMR has no confirmation message for user's security action, it does not inform users that their action can result in drastic and destructive consequences. DHIS2, with a defined set of roles and modification of security action to inform user action, has destructive consequences on data loss and access. On the other hand, SmartCare summarizes changes and show validity issues of sensitive data and give user option to go forward or to revise their security action.

In all three applications, security actions are grouped in a similar location, and function keys that can cause serious consequences are located at a hard-to-reach position. SmartCare even has a graphical keypad on the screen that allows users to use the mouse as a keyboard function. DHIS2 only display denied access for invalid function keys.

All three applications have no security warning messages for the user that they are about to do a potentially serious security error. In contrary to prevent a user from security errors, no feature found to inform in OpenEMR and disabled by default. DHIS2 displays and highlighted to be visible or accessible disabled to prevent security errors. No blocking mechanism nor warnings of security error found in SmartCare.

4.2.4 Convey Features/Expressiveness

The expressiveness or the check whether security guides convey features of the e-Health system, investigate how users are given the necessary guidance on security in a way that still gives them freedom of expression (Yeratziotis, Pottas, & Greunen, 2012). Users are respondents, not imitators of security actions for OpenEMR and SmartCare applications, but DHIS2 users are security initiators and sometimes act as respondents. Accordingly, no prompt for next security-related activity correctly anticipated by all three applications.

The security state of the system and alternatives for security-related actions were not available for users. DHIS2 displays a summary of a user account setting for the current user. In contrast, SmartCare presents a login control box highlighted with a blue outline and cursor blinking in the username text field. Labels are self-explanatory with ease of understandability, but the understanding of the security capabilities by users differs based on the technical knowledge they have.

4.2.5 Learnability

Learnability examines how the e-Health system ensures that security actions are easy to learn and remember by users (Kainda, Fléchais, & Roscoe, 2010). Similar actions are grouped into logical zones in sequence with headings to distinguish them in the three applications. The relationships between security controls and security actions are mapped apparently for users and are preconfigured by the system administrator in the case of OpenEMR.

Security operations of all three applications are easy to learn because they are in simple, clear, low-level language and labels are mapped logically with descriptions for users. Default security selection was not available instead, default values are prefilled for OpenEMR and DHIS2 applications; but SmartCare only presents the login controller box at the start of the application. GUI menus are well explained with default values that make which security items are selected obvious, DHIS2 is even considered the next action entries done by users.

Users are not protected from making severe errors in OpenEMR, but DHIS2 warn users about consequences, and SmartCare only provides a yes or no option confirmation to guide users before proceeding with changes. Some standards are followed to present security-related information like text pop-ups and welcome windows with the login control box in the case of DHIS2 and SmartCare, but OpenEMR has no information about the security.

4.2.6 Aesthetics and Minimalist Design

The aesthetics and minimalist design investigate how e-Health system security actions have relevant and related information for the users (Nielsen, 1994). Security Information that is essential to decision displayed with informative messages for all applications, OpenEMR, the security information assists users to make an appropriate decision, SmartCare integrates into one interface, but knowledge of the system is needed to understand displayed information.

All security icons are minimal and distinct for all applications visually and conceptually, in the case of SmartCare symbols and font color used for warnings and security actions. Security labels are described clearly and simply for DHIS2 and SmartCare. Besides, security prompts are expressed in positive and common yes, no, cancel options in SmartCare application.

4.2.7 Errors

Studying Error messages from e-Health systems helps to understand whether systems provide detailed security error messages that users can understand and act upon expressions (Yeratziotis, Pottas, & Greunen, 2012). OpenEMR and DHIS2 security-related messages sated constructively, with detailed descriptions that are highlighted in red without criticizing to help do a neat action. But SmartCare has not that many comments about security-related prompts. The error severity of security-related error messages was not described by any of the three applications in the study. The cause of problems in security-related error messages was not suggested by OpenEMR and DHIS2 applications rather, only current status was presented. In the case of SmartCare, there was no option found in the application to suggest the causes of problems.

The action needed by users to take a corrective measure was not fully explained in error messages of security-related actions but general and few errors were described in OpenEMR and DHIS2, but SmartCare had no security-related messages for users. The security-related error messages of all three applications were general and accurate in their descriptions without specific details of error messages.

4.2.8 Satisfaction

The satisfaction criteria of the e-Health system try to investigate how the system ensures that users have a good experience when using security and that they are in control (Yeratziotis, Pottas, & Greunen, 2012). The three applications have commonality not to have individual security setting as a member of family security options rather they all have individually predefined security and access without hierarchy nor inheritance.

To draw attention and indicate status on the change of security-related actions, information was presented in DHIS2 highlighted in red, and SmartCare with the login (green) and close (red) were used. On the other hand, users are not in control of security-related prompts that imply for all three applications.

4.2.9 User Suitability

The aim of user suitability evaluation for the e-Health system is to understand how the system provides options for users with diverse levels of skill and experience in security (Nielsen, 1994). It was found that all three applications do not have multiple levels of security error message detail. In the case of OpenEMR, predefined security and access control were managed through system administrator. Users have no option to choose between iconic and text display of security information in all applications other than the predefined options by default. Multiple levels of security detail were not available but only predefined security and access were available. For DHIS2 and OpenEMR, any privileged user was allowed to access security features.

Only elevated or privileged users can change their level of the security detail in OpenEMR and DHIS2 applications. Similarly, users without the right privilege cannot change between novice and expert levels, and also cannot customize security to meet their individual preferences, therefore they have to use only predefined preferences set by the system administrator.

4.2.10 User Language

User language is a criterion used to investigate how it is used to explain user with details they can easily understand about security controls (Yeratziotis, Pottas, & Greunen, 2012). OpenEMR and DHIS2 found to have security actions and objects named consistent across all prompts in their design.

Security information in DHIS2 found to be accurate, complete, and understandable by the users, but OpenEMR was found to partially fulfill this. With regards to security questions, all three applications stated in clear and simple language easily understandable by users. No privacy statement found in OpenEMR and DHIS2 application and security jargon was not discovered on OpenEMR and DHIS2.

4.2.11 User Assistance

While checking user assistance of the e-Health system, it was tried to investigate how security help is apparent for users of the system in the study (Yeratziotis, Pottas, & Greunen, 2012). Security help function was visible and found as an online or offline user manual for OpenEMR and DHIS2

applications. OpenEMR and DHIS2 found to have a piece of security information that was relevant but not sufficient. Users can easily switch between security help and their work for both applications because security help can be opened in a separate window/new tab.

Instructions follow the logical sequence of the user's security actions. The sequence of the help text was in line with the security feature in OpenEMR, and DHIS2 applications. User manual and online hyperlink were available for general exploration sites to get all the necessary help for users. The help in OpenEMR was found to be limited to explain unlike DHIS2, which gives an explanation and online links for further general explanations. No education option found in the SmartCare application.

4.2.12 Identity Signal

The identity signal for the e-Health system is used to examine valid certificates, and the information should be available on the browser of use (Yeratziotis, Pottas, & Greunen, 2012). OpenEMR and DHIS2 found to have display warnings and alerts of trustworthy sources in their browser, even if they do not interact with external sites, and the predefined setting was managed by their administrators.

Identity signal found to include human-readable information about the certificate subject for OpenEMR and DHIS2 applications, whereas in SmartCare certification was not found. Also, the identity signal found to include the issuer fields' organization attribute to inform the user about the party responsible for that information for both OpenEMR and DHIS2 applications.

4.2.13 Security and Privacy

Security and privacy criteria for the e-Health system help to investigate how the system considers integrity, availability, confidentiality, and privacy (Yeratziotis, Pottas, & Greunen, 2012). Protected areas found to be completely inaccessible for users without security privilege. Furthermore, predefined security and access groups with protected fields were hidden and inactive by the administrator in OpenEMR and DHIS2 applications. Administrators with a certain password and access level have the right authority to access protected and confidential areas in all three applications.

It was found that OpenEMR and DHIS2 have no consent regarding the use of users' personal information. Besides, there were no clearly stated purposes of users' personal information by all three applications. DHIS2 was found to allow users to modify their personal information, but in OpenEMR, the only administrator is allowed to update or delete inaccurate personal information. All of the three applications don't fulfill the measures that should be used to protect sensitive personal information users must provide. OpenEMR and DHIS2 were found to have a role-based definition for users to grant access, based on valid authorization.

Users were not notified of their access privileges in all three applications. With predefined security and access informative (OpenEMR), successful login and summary of users (DHIS2), happens when users try to access some element without privilege (SmartCare). Only DHIS2 found to have time-bound session lockout after a period of inactivity or upon user request. OpenEMR and SmartCare have setup sessions set by the system administrator and have no automatic lockup timeout.

DHIS2 enforced to limit consecutive attempts by the user during a period. Whereas in OpenEMR this was configured by an administrator and does not enforce to limit login attempts but for SmartCare, attempts were unlimited. Notification messages related to security and privacy are displayed for a user during the first attempt to access the application in only in the case of SmartCare.

SmartCare was found not to ensure that publicly accessible information does not contain nonpublic information. Software updates were notified before it is installed for OpenEMR and DHIS2 applications, but not in SmartCare as updates were installed centrally.

DHIS2 was found to have notification function, and SmartCare had only validation control as an automated tool for the users upon discovering discrepancies during integrity verification. No procedure for loss or duplication of personal information was established in OpenEMR and DHIS2 applications. Administrators perform reporting of security incidents in the case of OpenEMR through the official website. On the other hand, an administrator can configure mail or SMS to send security incidents and flaws in the case of the DHIS2 application.

OpenEMR and DHIS2 users are not allowed to back up their personal information, and only administrators can do this task if the need arises. Also, there was no backup policy that regulates how copies of information taken and tested regularly.

The user manual was available offline or online to provide awareness and educate the user to complete tasks in OpenEMR and DHIS2 applications. Enforcing minimum password complexity of defined requirements is done by the administrators of DHIS2, found that user-defined and enforce the complexity and minimum requirements, in the case of SmartCare users, are allowed to decide, OpenEMR users were not allowed to change password. Passwords were encrypted in storage for OpenEMR and DHIS2 applications. Administrators configure minimum and maximum password lifetime restrictions in OpenEMR and DHIS2 applications. Reuse for a defined number of generations was prohibited in the DHIS2 application, and SmartCare does not have password history. Confirmations for change were available in SmartCare users to understand, indicating the conditions of access.

4.3 Analysis and Presentation-Part-2

In this section, the second part of data analysis of thirteen criteria's or principles is presented based on the agreement or disagreement. Which were calculated as one-person say account to be 33.33 % of agreement or disagreement on each category and sub category. Furthermore, cumulative result was also calculated by adding all percentage and divide with the number of sub-categories of checklist of three experts on each e-Health applications derived from (Appendix F) is presented in detail as follows:

OpenEMR, evaluation of experts' agreement on compliance or not comply for each sub-criteria, taken into consideration if two experts agree or disagree on a given principle that the application complies or not. The cumulative of individual security heuristics shows that eight out of thirteen found to comply, as shown in table 4.1.

Table 4. 1 OpenEMR, experts' agreement on Security Heuristics

Security Heuristic Checklist	OpenEMR	
	Comply	Not Comply
1. Visibility	75%	16.67%
2. Revocability	27.78%	50%
3. Clarity	50%	33.33%
4. Convey Features/Expressiveness	33.33%	50%
5. Learnability	61.91%	38.38%
6. Aesthetics and Minimalist Design	100%	0%
7. Errors	60%	40%
8. Satisfaction	22.22%	66.67%
9. User Suitability	0%	72.23%
10. User Language	84.34%	11.11%
11. User Assistance	60%	40%
12. Identity Signal	73.33%	13.33%
13. Security and Privacy	22.22%	64.20%

DHIS2, evaluation of experts' agreement on compliance or not comply for each sub-criteria, based on expert's agreement on a given principle that it comply or not is presented in detail shown in table 4.2. The cumulative of individual security heuristics reviled that eight out of thirteen found to comply and one is not applicable to say comply or not comply due to the agreement found to be equal, shown (Appendix F).

Table 4. 2 DHIS2, experts' agreement on Security Heuristics

Security Heuristic Checklist	DHIS2	
	Comply	Not Comply
1. Visibility	33.33%	58.34%
2. Revocability	44.44%	55.56%
3. Clarity	25%	66.67%
4. Convey Features/Expressiveness	33.34%	50%
5. Learnability	90.48%	9.52%
6. Aesthetics and Minimalist Design	100%	0%
7. Errors	66.67%	33.33%
8. Satisfaction	44.45%	55.55%
9. User Suitability	0%	66.67%
10. User Language	83.34%	5.55%
11. User Assistance	46.67%	26.66%
12. Identity Signal	33.33%	13.33%
13. Security and Privacy	45.68%	32.10%

SmartCare, evaluation of experts' agreement on comply or not comply for each sub-criterion, presented in detail shown in table 4.3. Experts agreement on a given principle that SmartCare complies or not. The cumulative of individual security heuristics reviled that only four out of thirteen found to comply and one is found to be not applicable, shown in (Appendix F).

Table 4. 3 SmartCare, experts' agreement on Security Heuristics

Security Heuristic Checklist	SmartCare	
	Comply	Not Comply
1. Visibility	41.67%	50%
2. Revocability	22.22%	50%
3. Clarity	58.34%	33.33%
4. Convey Features/Expressiveness	25%	66.67%
5. Learnability	76.19%	23.81%
6. Aesthetics and Minimalist Design	83.33%	16.67%
7. Errors	40%	60%
8. Satisfaction	33.33%	44.45%
9. User Suitability	5.55%	61.11%
10. User Language	94.45%	0%
11. User Assistance	20%	26.67%
12. Identity Signal	0%	46.67%
13. Security and Privacy	28.39%	51.85%

Overall summary of three e-Health applications with color coding and classification is presented in detail with the description shown in table 4.4, further discussion is presented in chapter five on each category.

Table 4.4 Color description;

- Experts agree for ALL e-Health applications, comply with the criteria.
- Experts agree for TWO e-Health applications, comply with the criteria.
- Experts agree for ALL e-Health applications, not comply with the criteria.
- Experts agree for TWO e-Health applications, not comply with the criteria.
- Experts agree only ONE e-Health applications, comply or not comply on the criteria

Table 4. 4 Categorical Cumulative of experts' agreement for all three e-Health applications

Comply	OpenEMR	DHIS2	SmartCare
1. Visibility	75%	33.33%	41.67%
2. Revocability	27.78%	44.44%	22.22%
3. Clarity	50%	25%	58.34%
4. Convey Features/Expressiveness	33.33%	33.34%	25%
5. Learnability	61.91%	90.48%	76.19%
6. Aesthetics and Minimalist Design	100%	100%	83.33%
7. Errors	60%	66.67%	40%
8. Satisfaction	22.22%	44.45%	33.33%
9. User Suitability	0%	0%	5.55%
10. User Language	83.34%	83.34%	94.45%
11. User Assistance	60%	46.67%	20%
12. Identity Signal	73.33%	33.33%	0%
13. Security and Privacy	22.22%	45.68%	28.39%
Not Comply			
1. Visibility	16.67%	58.34%	50%
2. Revocability	50%	56.56%	50%
3. Clarity	33.33%	66.67%	33.33%
4. Convey Features/Expressiveness	50%	50%	66.67%
5. Learnability	38.38%	9.52%	23.81%
6. Aesthetics and Minimalist Design	0%	0%	16.67%
7. Errors	40%	33.33%	60%
8. Satisfaction	66.67%	55.55%	44.45%
9. User Suitability	72.23%	66.67%	61.11%
10. User Language	11.11%	5.55%	0%
11. User Assistance	40%	26.66%	26.67%
12. Identity Signal	13.33%	13.33%	46.67%
13. Security and Privacy	64.20%	32.10%	51.85%

4.4 Summary

In this chapter, the collected data from the participant was organized and analyzed to be ready for presentation and interpretation. The analysis and presentation have two parts. The first part presented the thematic analysis and the second part presented the experts' agreement and disagreement on each criteria whether they compliance or non-compliance on each e-Health applications.

The next chapter will present the discussion part of the study on the data analysis and presented in chapter four.

Chapter Five

Discussion

The purpose of the study was to evaluate the usability of security mechanisms of e-Health applications and based on the finding to propose recommendations for current as well as for future development of e-Health applications to give more attention on the usability aspect of security mechanisms with consideration of novice or expert users in the health domain. The security heuristic checklist based on concepts of usability and security aspects, derived from the literature, was used in the evaluation of the selected e-Health application. The result of the evaluation using these checklist criteria are discussed in the section below. The discussion presents how the three e-Health applications comply with, based on the three experts' evaluations. In this section, results are discussed using the existing relevant literature. The first part of the discussion starts with security heuristics that comply and latter security heuristics that did not comply accordingly.

5.1 Security Heuristics Compliance

All of the three e-Health applications, according to the experts' evaluation, were found to comply with these three security heuristics namely, *Learnability*, *Aesthetics,* and *Minimalist*, and *User Language*.

Learnability

In using certain e-Health applications the authentication steps should be easy enough to learn and to remember by users (Al-Sarayreh, Hasan, & Almakadmeh, 2015). The experts' evaluation of using the learnability criteria indicated that the three applications comply, which implies these e-Health applications were found to be easy to learn and remember for users. In supporting their judgment the experts were making the following remarks, for example, Exp.1 commented "*These settings are either access denied or hidden from the users. DHIS2 allows for multiple users to access the system simultaneously, each User is a member of a defined set of Roles with defined permissions*." Also, Exp.2 commented, "*Similar actions are grouped and sequenced logically in tabs and with a brief explanation for each* and *the simple titles and the mapping of individual function keys for the simplest action possible action, promotes easy learning"*. Moreover, Exp.3

commented, "*No vague language of the security word is clearly stated in low-level understanding*". All of the experts were agreed that the security operations were easy to learn and use, these implied that security operations use a simple title with clear language and descriptions for the users.

In another similar study, indicated that ease-of-learning which measures the ease in learning use of security or privacy features, also ease in remembering features after not using them for a time. One of the application scored very good, while the other one scored barely acceptable‖ by using different research approach (Yeratziotis, Greunen, & Pottas 2011).

Aesthetics and Minimalist

Only relevant information should be visible in the system security mechanisms, without overwhelming the user with information, the number of settings, passwords to remember (Fierro & Zapata, 2016). The evaluation of aesthetics and minimalistic criteria indicated that comply with the three applications, relevant security actions were observed to inform users (Pierotti, 2005). Exp.1 indicated with a screenshot of DHIS2, all security icons in a set visually and conceptually distinct, shown in Fig 5.1 below.

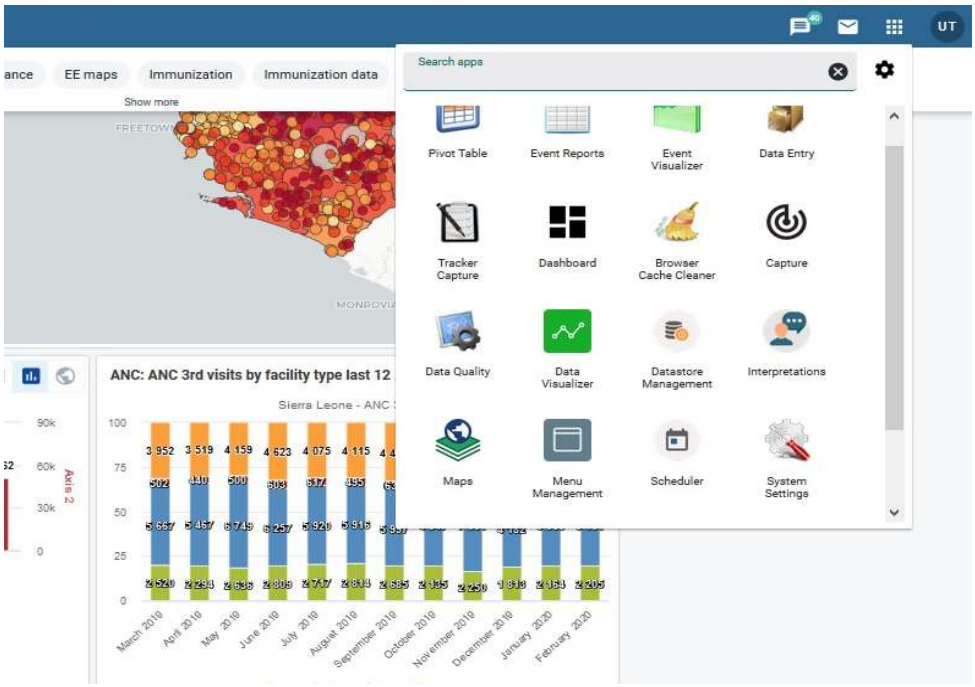


Figure 5. 1 Screenshot of DHIS2 application by Exp.1

Besides, Exp.2 commented, "*If/When present, informative messages are displayed in a way that assists the user to make decisions on the action they are about to perform*." Security-related information that would affect the decision of security action should be presented clearly for the users (Pierotti, 2005). Also, security labels should be visually and conceptually district icons with clear descriptions (Pierotti, 2005).

User Language

User language criteria, the system should use language which is easy to understand for the users (Yeratziotis, Pottas, & Greunen, 2012), based on the expert's evaluation indicated that it complies with the heuristic checklist indicated Exp.2 commented, "*There are no jargons related to security*". Also, Exp.3 stated, "*the security actions and security objects are shown consistently across all prompts*". Security should use language appropriate for users, simple, clear that can be understood easily (Hausawi, Allen, & Bahr, 2014). Besides, the system should avoid any unnecessary technical jargon and confusing acronyms (Akash, & Janet, 2009).

As indicated in the evaluation the design of security action, object, and information should be consistent, accurate, complete, and in simple language across all. Similarly, one study showed that terminology which measures the logical, natural order of information. It uses phrases and concepts familiar to users and avoids complicated security or privacy terms. On the study, both website applications scored very good and good. However, barely acceptable and poor ratings also occurred (Yeratziotis, Greunen, & Pottas 2011).

On the other, OpenEMR and DHIS2 applications found to comply for these three security heuristics, which are *Errors*, *User Assistance*, and *Identity Signal*, discussed as follows:

Errors

The study shows that error messages should prevent users before the error occur and present or prompt the users for their confirmation (Nielsen, 1994). These messages should be polite, precise, humane readable and constructive to reduce the work required to fix the problem and educate user

along the way, for example, “404 error message “ web most common error violates most of these guidelines and recommended for custom error message “page not found” (Nielsen, 1994).

Experts’ evaluation of the criteria of errors showed that OpenEMR and DHIS2 e-Health applications comply with this heuristic criterion. Comment of Exp.2 stated, “When *error message was displayed, in a constrictive, descriptive and accurate way*”. Errors messages should inform its severity, its cause, and corrective actions for users to understand them well and act appropriately (Pierotti, 2005).

User Assistance

The system help should be able to assist users when there is a need arises and at the same time educate them along the way for security-related activities (Yeratziotis, Pottas, & Greunen, 2012).

The experts’ evaluation of OpenEMR and DHIS2 on the criteria of user assistance indicated they comply with this heuristic. Two of the three experts commented, “*Online/offline User manual is availed* and *there is an online help/manual with explanations for security features*”. Security help for users should be able to assist users in such a way that security help information was visible, relevant, and educational (Akash, & Janet, 2009).

Identity Signal

Valid certificate and information about the certificate should be available for the users while using an application on the browser (Yeratziotis, Pottas, & Greunen, 2012). Based on the experts’ evaluation for the criteria of identity signal observed at OpenEMR and DHIS2, applications they comply with this heuristic. Two of the three experts agreed on their comment, “*the identity signal includes readable information about the certificate subject which also includes the advises that user will do*”. Information about the validity of certificates should be available for users are using a secure way of communicating with the system they use (Yeratziotis, Pottas, & Greunen, 2012).

In similar, OpenEMR and SmartCare, applications were found to comply for the Clarity of security heuristics are presented below:

Clarity

Good error messages should be designed carefully, which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action (Nielsen, and Mack, 1994).

The experts' evaluation of clarity criteria revealed that OpenEMR and SmartCare applications comply with the standard. Stated by Exp.2 "*all function keys were located on a similar location for all security actions of a user*". Also, Exp.3 "*such kinds of messages are displayed and highlighted to make it visible/accessible for the user*". Clarity as a criterion aimed to increase users' understanding of the communication of security actions by informing uses in advance about the consequences of any security action (Nielsen, 1994). Prompts, warnings, notifications are e-System communication means to provide information to users, but this information should be simple and clear to be understood by novice users (Nielsen, 1994).

On the other hand, these e-Health applications have similar function keys for security were grouped in a similar location, these make it clear for the users to easily locate and remember them (Nielsen, 1994). User action and its consequences should give proper warring feedback clearly (Capilla, Carvajal, & Lin 2014).

One of the e-Health applications found to comply with one or two of the security heuristics criteria is discussed below respectively; OpenEMR comply *Visibility*, DHIS2 comply *Satisfaction* and *Security and Privacy.*

Visibility

OpenEMR found to comply with this criterion based on expert evaluation. An appropriate user security login provides security-related error messages that displayed next to the field where the user committed an error (Nielsen, 1994 & 2001). Fig 5.2 shows a screenshot of OpenEMR

windows with an error message clearly. Besides, Exp.2 commented, "*Only error details are explained in plain text*".

The e-Health application should provide a feedback message indicating that the subsequent collection of the task needs to be started (Nielsen, 1994). The expert also revealed in their evaluation that the application offers feedback for each security-related incident (Nielsen, 1994). A study shows that pop-up windows should display an error message with apologetic means significantly decrease users' frustration (Park et al., 2012).

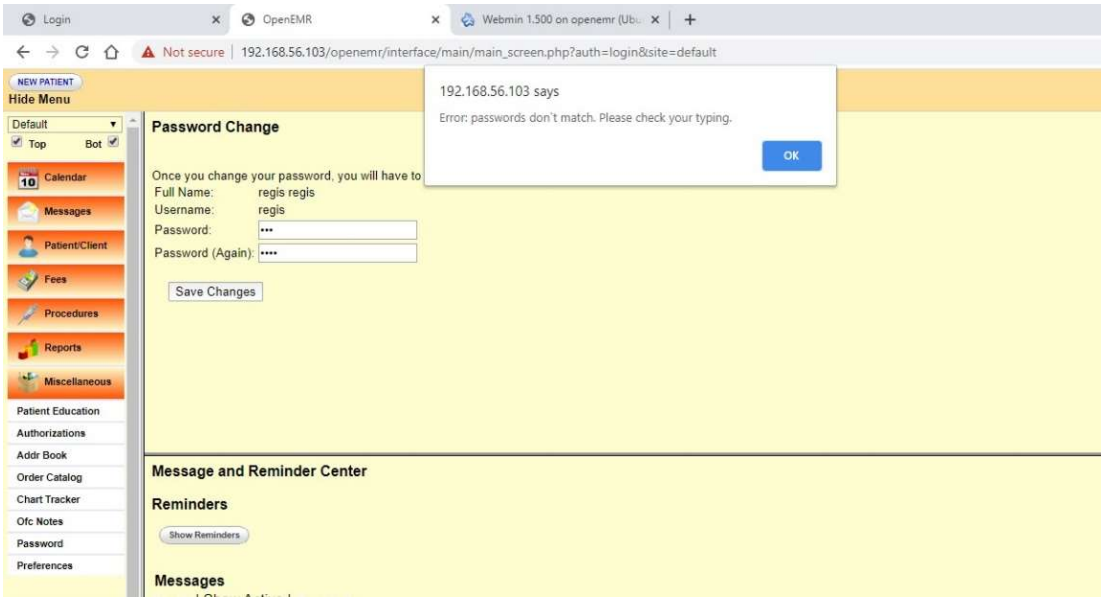


Figure 5. 2 Screenshot of OpenEMR by Exp.1 Visibility with the error message.

Satisfaction

DHIS2, the only application that complies the security heuristics in a way that each security setting a member of a family of security options are grouped and represented with color to draw attention, shown in Fig 5.3. The overall system of user satisfaction was determined by the combination of the user satisfaction values of its components (Norman, 1983).

Security setting should be a member of a family of security options and differentiated with consistent color throughout the system, ease of understanding for users' attention and changes for

security-related actions and information security setting were a member of a family of security (Pierotti, 2005).

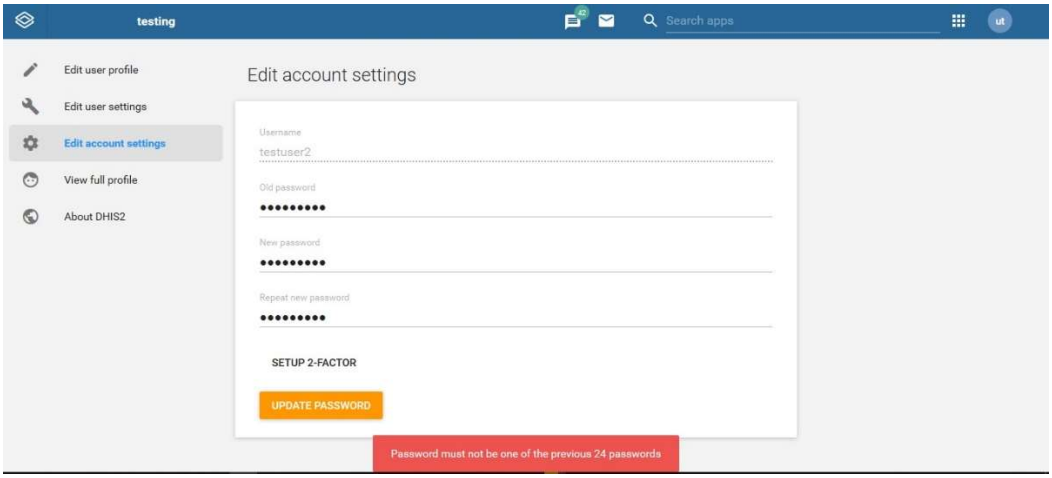


Figure 5. 3 Screenshot by Exp.1 shows group and coloring interface of DHIS2.

Security and Privacy

Integrity, availability, confidentiality, and privacy should be considered for the criteria of security and privacy with security-related activities (Yeratziotis, Pottas, & Greunen, 2012). Breach of sensitive e-health data would severely cause threats leading to tampering of health and personal related information. So preserving the privacy of the patient information is an important feature in e-health systems (Sahama, Simpson, & Lane 2013). Based on the experts' evaluation of the security and privacy criteria indicated DHIS2 complies with the heuristic criteria. For example, two of the experts out of three commented, "*protected areas are completely inaccessible, the backend/confidential areas of the system can be accessed with passwords, session lockout with specific time-bound, enforce the minimum requirement and complexity of the password*, *passwords are encrypted in storage,* and *users can modify only their information*".

5.2 Security Heuristics noncompliance

In this section, all three e-Health applications did not comply with security heuristics of Revocability and *User Suitability,* discussed in detail.

Revocability

Revocability was included in user control and freedom of Nielsen's ten heuristics, users often choose system functions by mistake and will need a marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo (Nielsen, 1994).

Based on the experts' evaluation of revocability showed none of the three e-Health applications comply with this heuristic criteria, stated by the experts' "*no Undo buttons to reverse security action, means to terminate an act in the middle of an operation or in-progress*". The method that enables users to de-selection a security option gives users a chance to correct security action, and notification of the correction visually communicated to notify users that the error was reverted (Nelson, 1994).

The user of e-Health application can do a security action error unintentionally or intentionally, to take correction, reverting method should be available to facilitate the action (Nelson, 1994). Not all three applications have an "undo" button or means of termination of security action on progress. Undo function should help users to reverse their actions and clear, consistent message with GUI menus regarding the reversing action successfulness (Pierotti, 2005). The expert revealed in their evaluation that the applications were not able to revoke any of the security-related actions by users (Nelson, 1994).

User Suitability

Users at a different level should use the system with their level of skills and experience in security (Yeratziotis, Pottas, & Greunen, 2012). Also, the system should support customization to their level of user preference (Akash & Janet, 2009). All of the three e-Health applications were not to comply with the criteria of user suitability. For instance, Exp.1 and Ex2 commented, "*User is a member of a defined set of Roles with Security & Access Control Groups of permissions*". Users with different levels of skill and experience in security should have options that are appropriate with their level of understanding of the security-related actions (Yeratziotis, Pottas, & Greunen, 2012).

OpenEMR and SmartCare were found not comply with the security heuristics of *Convey Features/Expressiveness*, *Satisfaction*, and *Security and Privacy*. They are discussed in this section as follows.

Convey Features/Expressiveness

The system should convey relevant messages to guide users on security and freedom of expression (Yeratziotis, Pottas, & Greunen, 2012). The user interface of the authentication screen should convey the available security feature clearly and appropriately (Mendoza-González, Martin, & Rodríguez-Martinez, 2011).

Based on the experts', the evaluation of Convey Features/Expressiveness indicated that there is no prompting for next security action, no description of the security state, and users are not initiators of security actions. Comment of Exp.2 indicated, "*It is not observed on the system for a prompt or showing a message for next action expected from users* and *different security capabilities, most of them are not readily understandable by all users. Hence, a technical person can easily understand them but not in the case of non-technical*". Besides, security capabilities were not easy for non-technical persons to understand it well. Users should be able to view the security features and their capabilities and act if appropriate (Neilson, 1994).

The e-Health system should be able to propose the next security action, security state, and clear information on security capabilities for the users (Pierotti, 2005). Accordingly, OpenEMR and SmartCare applications do not comply with the criteria.

Satisfaction

The overall system user satisfaction is determined by the combination of the user satisfaction values of the system components (Norman, 1983).

One of the experts commented, "*No hierarchical security relationship is available. No inheritance of security setting is also included in any of the security settings. No distinct coloring is implemented for security-related changes. There are no prompts that are related to security.*" Security setting should be a member of a family of security options and differentiated with

consistent color throughout the system, ease of understanding for users' attention and changes for security-related actions and information security setting were a member of a family of security (Pierotti, 2005). Based on the experts' evaluation for the satisfaction criteria OpenEMR and SmartCare do not comply.

Security and Privacy

Breach of sensitive e-Health data would severely cause threats leading to tampering of health and personal related information. So preserving the privacy of the patient information is an important feature in e-health systems (Sahama, Simpson, & Lane 2013). Based on the experts' evaluation OpenEMR and SmartCare not comply with the security and privacy criteria indicated by the experts' comment, All the experts commented, "*Users are members of a predefined Security & Access Control Groups. There is no lifetime restriction on the passwords. The user can reuse the password without any limited time. No Password history maintenance with unlimited Attempted* and *the system will not lock with specific time-bound unless the user lockout it."* Also, "*No consent is requested from users about the information they provide. Backups are available as an integral part of the system but there is no policy about how copies of such information will be utilized." Furthermore, "no notification on the access privileges.*

On the other hand, DHIS2 and SmartCare applications found not comply with the *Visibility* criteria, which were discussed as below:

Visibility

Based on the experts' evaluation of visibility criteria indicated that there is no significant delay is observed in the three applications until the user is to perform the next security action, brief delay for each failed attempts and a long delay for several failed login attempts were used as a security measure from brute force login attacks (Cobb et al., 2015). An appropriate user security login provides security-related error messages that will be displayed next to the field in where the user committed an error (Nielsen, 1994 & 2001), from this end all the three e-Health application does not comply the specified criteria.

The e-Health applications, once the expert finalized a security action, the application should provide a feedback message indicating that the subsequent collection of the task needs to be started (Nielsen, 1994). On the other hand, DHIS2 and SmartCare do not have such a feedback feature for what to do next once a successful login is accomplished. The expert also revealed in their evaluation that the application offers feedback for each security-related incident (Nielsen, 1994). A study shows that pop-up windows should display an error message with apologetic means significantly decrease users' frustration (Park et al., 2012). But in this study Exp.2 commented, "*There are no pop-up windows for security-related issues or there was no security action completion feedback, it won't indicate specific fields but data entry boxes that resulted in the errors*." Exp.3 also added "*When you enter a correct username but wrong password though the system does not specify the error is username or password. If the username is correct, it shouldn't be requested again.*"

The remaining security heuristics were found to be not complied for each of e-Health applications; DHIS2, not comply with *Clarity,* SmartCare*, not comply Error* and *Identity Signal.* Here is the discussion on them:

Clarity

The clarity of error messages is essential for the users to understand the consequences of their security actions before they commit to the action *(*Nielsen, & Mack, 1994). The experts' evaluation of clarity criteria reviled DHIS2 does not comply. Comment by Exp.2 states," *They are not displayed and/or when clicked access is denied*." Clarity as a criterion aimed to increase users' understanding of the communication of security actions by informing uses in advance about the consequences of any security action (Nielsen, 1994). Prompts, warnings, notifications are E-Systems' communication means to provide information to users, but this information should be simple and clear to be understood by novice users (Nielsen, 1994). But in this study, the experts showed that these e-Health applications do not have a security warning before making security error, blocking mechanisms for prevention, and confirmation prompt. Even the application has no means to prevent users from making security errors according to experts. User action and its consequences should give proper warring feedback clearly (Capilla, Carvajal, & Lin, 2014).

Errors

One study shows that error messages should prevent users before the error occur and present or prompt the users for their confirmation (Nielsen, 1994). These messages should be polite, precise, humane readable and constructive to reduce the work required to fix the problem and educate user along the way, for example, “404 error message “ web most common error violates most of these guidelines and recommended for custom error message “page not found” (Nielsen, 1994).

Experts’ evaluation of the criteria of errors showed that SmartCare does not comply. Errors messages should inform its severity, its cause, and corrective actions for users to understand them well and act appropriately (Pierotti, 2005).

Another study indicated that, errors measures difficulties for users with security, and if errors occur, the problem and its solution must provide with plain language so that users can manage the error. Their result showed both website applications scored low and averaged, which are barely Acceptable (Yeratziotis, Greunen, & Pottas 2011).

Identity Signal

Valid certificate and information about the certificate should be available for the users while using an application on the browser (Yeratziotis, Pottas, & Greunen, 2012). Based on the experts’ evaluation for the criteria of identity signal observed that SmartCare does not comply. Information about the validity of certificates should be available for users are using a secure way of communicating with the system they use (Yeratziotis, Pottas, & Greunen, 2012).

5.3 Key Findings

The study findings show that most of the security heuristic checklist found to be noncompliance with these three e-Health applications based on the expert's review. However, all of the three applications comply with three of the security heuristics and not comply with two of the security heuristics. Furthermore, DHIS2 complies with eight of the security heuristics, and SmartCare complies with four of the security heuristics.

Revocability and User Suitability of security heuristics do not comply with all e-Health applications in this study. On the other hand, Learnability, Aesthetics, and Minimalist Design happen to comply with all e-Health applications shown in table 5.1.

Table 5. 1 Compliance or noncompliance with the security heuristics.

Comply	OpenEMR	DHIS2	SmartCare
5. Learnability	61.91%	90.48%	76.19%
6. Aesthetics and Minimalist Design	100%	100%	83.33%
10. User Language	83.34%	83.34%	94.45%
3. Clarity	50%	25%	58.34%
7. Errors	60%	66.67%	40%
11. User Assistance	60%	46.67%	20%
12. Identity Signal	73.33%	33.33%	0%
1. Visibility	75%	33.33%	41.67%
8. Satisfaction	22.22%	44.45%	33.33%
13. Security and Privacy	22.22%	45.68%	28.39%
2. Revocability	27.78%	44.44%	22.22%
4. Convey Features/Expressiveness	33.33%	33.34%	25%
9. User Suitability	0%	0%	5.55%
Not Comply			
2. Revocability	50%	56.56%	50%
9. User Suitability	72.23%	66.67%	61.11%
1. Visibility	16.67%	58.34%	50%
4. Convey Features/Expressiveness	50%	50%	66.67%
8. Satisfaction	66.67%	55.55%	44.45%
13. Security and Privacy	64.20%	32.10%	51.85%
3. Clarity	33.33%	66.67%	33.33%
7. Errors	40%	33.33%	60%
12. Identity Signal	13.33%	13.33%	46.67%
5. Learnability	38.38%	9.52%	23.81%
6. Aesthetics and Minimalist Design	0%	0%	16.67%
10. User Language	11.11%	5.55%	0%
11. User Assistance	40%	26.66%	26.67%

5.4 Summary

In this chapter, the discussion of the presented data done in detail for each security heuristic result for each e-Health application, based on the experts' comments and agreement.

Using the security heuristic checklist and experts, evaluation of the usability of security mechanisms of e-Health application on these three applications, OpenEMR, SmartCare, and DHIS2, pointed that the security mechanisms need improvement and future e-Health applications to consider and proper attention should be taken in account in the development stage by considering the usability aspect of security mechanisms.

Finally, the gaps and challenges for the usability of security mechanisms of e-Health applications on each security heuristic criteria have been identified.

Chapter Six

Conclusion and Recommendation

This chapter presents a conclusion, recommendations, and further studies for other researchers to pursue these topics intensely to explore or extend the existing study to the same or another domain.

6.1 Conclusion

The first research question of the study was to evaluate the usability of security mechanisms of e-Health applications that are being in use in Ethiopia. Evaluation of the usable security topic area is very hard and complex without a proper evaluation tool, which involves different fields of studies, such as security, usability, and human-computer interactions (Kainda, Ronald & Flechais, Ivan & Roscoe, 2010). The first challenge was how to evaluate the usable security of a given system, to identify suitable evaluations method and criteria.

After a rigorous literature review, the researcher found a framework for evaluating usable security in the health domain. The framework uses three phases to identify the higher level of security heuristics for the purpose evaluation method. These higher levels of a heuristic checklist are adopted for this study. Moreover, based on the evaluation framework, the evaluation of the usability of the security mechanisms of e-Health application in Ethiopia, done successfully.

The health sector in Ethiopia was implementing e-Health application systems throughout the health facilities to facilitate clinical data collection and dissemination using electronically (JSI, 2019; USAID, 2019). DHIS2 and OpenEMR applications are recent and open-source. On the other hand, SmartCare being the earlier application still in use in government health facilities. Many of these e-Health applications were developed in house or open-source and customized, furthermore, donor-funded projects.

The study result shows that the three e-Health application tends to comply for some criteria and not to comply on another criterion. For instance, OpenEMR, DHIS2, and Smart care all comply with these three criteria, *Learnability*, *Aesthetics and Minimalist Design*, and *User Language.* Also, OpenEMR and DHIS2 comply with these criteria, *Errors*, *User Assistance*, and *Identity Signal*. OpenEMR and SmartCare comply with the criteria of *Clarity.* OpenEMR complies with

Visibility criteria. Finally, DHIS2 comply with these two criteria's, *Satisfaction* and *Security and Privacy.*

The study result shows these e-Health applications do not comply with these two criteria's *Revocability* and *User Suitability.* Also, OpenEMR and SmartCare do not comply with these two criteria, *Convey Features/Expressiveness*, *Satisfaction* and, *Security and Privacy.* Moreover, DHIS2 and SmartCare also do not comply with *Visibility* criteria. Also, DHIS2 does not comply with the *Clarity* criteria. Finally, SmartCare also does not comply with these two criteria Errors and *Identity Signal*.

After the evaluation, the following findings are observed and identified for the e-Health applications selected for this study. Based on the analysis and findings, the following points are identified. This leads to answering the second question of this research, how to improve the usability aspect of security mechanisms. These criteria's were identified for improvement, which is as follows:

- **Revocability**

  It suggested that experts and some research from literature, the two-factor authentication method is a way forward to secure identity, data in storage and in-transit, data sharing using a cloud system, and making the revocability of the security mechanism is highly usable for the users (Liu, Liang, Susilo, Liu, & amp; Xiang, 2016; Sanjay, Dattatray, Bansi, & Yashawant, 2016).

- **User Suitability**

  An expert from this study suggested, clear and easy to understand security prompt error messages should improve it, for example, when the user changes a password, the error message should indicate a clear description with the cause and how to correct it immediately. Also, the system should be able to educate the users using the error prompt (Realpe, Collazos, Hurtado, & Granollers, 2016; Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016; (Jones, Keane, Stawiarski, Fatus, & Kane, 2016).

  Literature suggests that the legislative environment can play a crucial role in further growth of security (Barlette & amp; Fomin, 2008). Also, Hof (2012) suggested that the two guidelines improve the usability of security mechanisms discussed as follows:

Guide one “Understandability, open for all users” developer should design a means to hide many security mechanisms, also for the remaining features, the average end-users should get security awareness in addition to using easier, everyday life metaphors in simple word with powerful meaning. Example: an email encryption application should not use the term “encrypted email”. It is better to talk about a “secret message for XY” or “email readable only by XY” where XY is the receiver of the message.

Guide two “Empowered users” usable security mechanism should not restrict the user from their tasks, rather the absence of user restrictions often results in a better acceptance. The focus should be on protecting the user than restrict. Users should feel they are in control than the system controls them. Also the usual flow of activities in the least possible way.

“Security mechanisms are of great use for businesses, they constantly restrict the user, hence force him to bypass security mechanisms. As users are very imaginative in bypassing unwanted restrictions, it is very likely, that a non-security-motivated restriction decreases the security level of a system.” For example; iPhone enforces many restrictions, many users bypass the security mechanisms by using a jailbreak software to revoke those restrictions.

Therefore, these two guidelines should improve the user suitability as well as the usability aspect of the security mechanisms from design for security perspective.

6.2 Recommendations

The significance of security mechanisms for e-Health applications undeniable (Chenthara, Ahmed, Wang, & Whittaker, 2019). These mechanisms are in place to protect the privacy of personal and clinical data in the system without question (Institute of Medicine, 1994). In doing so usability aspect of security mechanisms, seems to be given less focus on the development of e-Health applications or in general any information system application (Al-Issa, Ottom, & Tamrawi, 2019). Therefore, for the security mechanism to be more secure, they should be usable too (Kainda, Ronald & Flechais, Ivan & Roscoe, 2010). Based on the study result, the researcher recommends giving due attention especially for the usability aspect of security mechanisms in the development of e-Health application SDLC. Besides, other recommendations are as follows in brief:

- System developers should give equal consideration for security and usability in the design phase to get a usable and secure application at the end (Flechais, Mascolo, Sasse, 2007).
- Security experts should involve usability experts to come up with a win-win application with usable security for the end-users (Gutmann & Grigg, 2005; Kainda, Fléchais, & Roscoe, 2010)
- The requirement gathering and analysis phase should incorporate the usability aspect of security mechanisms (Kainda, Fléchais, & Roscoe, 2010).
- Evaluation of usable security should be done before the implementation of any e-Health applications (Flechais, Mascolo, & Sasse, 2007).
- Policymakers should include the usability aspect of security mechanisms for the sensitive and critical data in the e-Health system not to violate privacy (Institute of Medicine, 2010; Gawlik, Kkster, Mahmoodi, & Winandy, 2014; Al-Issa, Ottom, & Tamrawi, 2019).
- User awareness training on security mechanisms, which they are there in place to protect them not to make their daily activity hard (Liska, 2015).

Pieces of literature evidence from (Flechais, Mascolo, & Sasse, 2007) underlined that giving equal consideration for security and usability in the design, the involvement of usability expert and security experts together to deliver secure and usable software (Gutmann & Grigg, 2005; Kainda, Fléchais, & Roscoe, 2010), Usability of security should be best treated in early SDLC phase (Kainda, Fléchais, & Roscoe, 2010), In general, to identify and rectify any usability issues of security a proper evaluation should be mandatory before implementation and after the correction measure done (Flechais, Mascolo, & Sasse, 2007), also policymaker should consider the usability aspect of security on the formulation of security policy (Institute of Medicine, 2010; Gawlik, Kkster, Mahmoodi, & Winandy, 2014; Al-Issa, Ottom, & Tamrawi, 2019). Security awareness training should be done periodically, users make proper and safe decisions on security issues (Liska, 2015).

6.3 Limitations of the Study

Research in the current pandemic of COVID19 is one big challenge. This study was designed to follow security heuristic checklist as a data collection methods for each e-Health application. And

also the evaluation process was completed beyond the estimated time of six days, two days for each e-Health application was dedicated, the third and the last data received took three weeks. Finally, two experts were not able to finalize the evaluation process due to personal reasons and they were omitted from the study.

6.4 Future Works

To deal with the current advance in a system security breach, threats, and risks of e-Health applications, the usability aspect of a security mechanism should be a rich topic area for further issues that are recommended for future research.

- Development of an easy tool for identification of usability issues of security early in the development stage.
- Identification of factors for the cause of usable security challenges.
- Security mechanisms challenges in e-Health applications.

References

Abouelmehdi, Karim & Beni-Hessane, Abderrahim & Khaloufi, Hayat. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data.5.10.1186/s40537-017-0110-7.

Ajami, S., & Bagheri-Tadi, T. (2013). Barriers for Adopting Electronic Health Records (EHRs) by Physicians. Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina : casopis Drustva za medicinsku informatiku BiH, 21(2), 129–134. https://doi.org/10.5455/aim.2013.21.129-134.

Akash S, Janet W (2009) Evaluation criteria for assessing the usability of ERP systems: Proceedings of the 2009 annual research conference of the South African Institute of Computer Scientists and Information Technologists: 87–95

Akhtar, I. (2016). Research Design. SSRN Electronic Journal. Doi: 10.2139/Ssrn.2862445

Alexandros Yeratziotis, Dalenca Pottas and Darelle Van Greunen (2012): A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm, International Journal of Human-Computer Interaction, DOI:10.1080/10447318.2011.654202

Alexandros Yeratziotis (2011): A Framework to Evaluate Usable Security in Online Social Networking. Ph. D in Information Technology in the Faculty of Engineering, the Built Environment and Information Technology of the Nelson Mandela Metropolitan University

Alka Agrawal, Mamdouh Alenezi, Dhirendra Pandey, Rajeev Kumar and Raees Ahmad Khan, (2019): Usable-Security Assessment Through A Decision Making Procedure. ICIC Express Letters Part B: Applications Volume 10, Number 8, August 2019 pp. 665-672

Al-Sarayreh, K. T., Hasan, L. A., & Almakadmeh, K. (2015). A Trade-Off Model of Software Requirements for Balancing Between Security and Usability Issues. International Review on Computers and Software (IRECOS), 10(12), 1157. DOI: 10.15866/irecos.v10i12.8094

Alshamari, M. (2016). A Review of Gaps between Usability and Security/Privacy. Int. J. Communications, Network and System Sciences, 9, 413-429.

Anwar, Fozia & Shamim, Azra. (2011). Barriers in Adoption of Health Information Technology in Developing Societies. Food Chemistry - FOOD CHEM. 2. 10.14569/IJACSA.2011.020808.

Atterer R, Wnuk M, Schmidt A. (2006): Knowing the User's every move - User activity tracking for Website usability evaluation and implicit interaction. In: Proceedings of the 15th International Conference on World Wide Web (Edinburgh, Scotland, May 23-26). New York, NY: ACM; p. 203-212.

Astalin PK. Qualitative Research Designs: A Conceptual Framework. Int J Soc Sci Interdiscip Res. 2013;2(1):118–24.

Basit TN. (2003). Manual or Electronic? The Role of Coding in Qualitative Data Analysis. Educational Research. 2003;45((2)):143–54.

Benantar, Messaoud. (2006). Access control systems. Security, identity management and trust models. Access Control Systems: Security, Identity Management and Trust Models. 10.1007/0-387-27716-1.

Bergaus, M., & Behringer, R. (2015). Design issues for service delivery platforms: Incorporate user experience: A grounded theory study of individual user needs. Heidelberg: Springer Vieweg.

Beverly Amunga Onyimbo and Babak Bashari Rad. (2016). Usability and Security in User Interface Design: A Systematic Literature Review. I.J. Information Technology and Computer Science, 5, 72-80.

Bourgeois, Dave, and David T. Bourgeois. (2014)."Information Systems Security." Information Systems for Business and Beyond. Ch. 6

Braa, Jørn & Hanseth, Ole & Heywood, Arthur & Mohammed, Woinshet & Shaw, Vincent. (2007). Developing Health Information Systems in Developing Countries: The Flexible Standards Strategy. MIS Quarterly. 31. 381-402. 10.2307/25148796.

Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a Trade-Off Between Usability and Security: A Metrics Based-Model. Lecture Notes in Computer Science Human-Computer Interaction – INTERACT 2007, 114-126. doi:10.1007/978-3-540-74800-7_9

Burton, L. C., Anderson, G. F., & Kues, I. W. (2004). Using electronic health records to help coordinate care. The Milbank quarterly, 82(3), 457–481. https://doi.org/10.1111/j.0887-378X.2004.00318.x

Carmines, E. G. & Zeller, R. A. 1979. Reliability and Validity Assessment, Newbury Park, CA, Sage.

Capilla, Rafael, et al. (2014) "Addressing Usability Requirements in Mobile Software Development." Relating System Quality and Software Architecture, 2014, pp. 303–324., DOI:10.1016/b978-0-12-417009-4.00012-0.

Chowdhury M., Jahan S., Islam R., Gao J. (2018). Malware Detection for Healthcare Data Security. In: Beyah R., Chang B., Li Y., Zhu S. (eds) Security and Privacy in Communication Networks. SecureComm 2018. Lecture Notes of the Institute for

Computer Sciences, Social Informatics and Telecommunications Engineering, vol 255. Springer, Cham

Clarke, V., & Braun, V. (2013). Teaching Thematic Analysis: Overcoming Challenges and Developing Strategies for Effective Learning. Psychologist, 26(2), 120-123

Cranor, L. F., & Garfinkel, S. (2005). Security and usability: Designing secure systems that people can use edited by Faith Lorrie Cranor and Simson Garfinkel. North Sebastopol, CA: O'Reilly Media. Ch.2, Page 21

Creswell, W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition. Sage, London.

Dalpiaz, F., Paja, E., & Giorgini, P. (2016). Security requirements engineering: Designing secure socio-technical systems. Cambridge, MA: The MIT Press.

Dave Bourgeois and David T. Bourgeois, (2014). Information Systems Development, ch 10 https://bus206.pressbooks.com/chapter/chapter-10-information-systems-development/

Derek Wiedenhoeft, (2019). HIPAA Compliance: Important Fundamentals You Need to Know. atlantic.net

Donald A. Norman. (1983). Design principles for human-computer interfaces. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '83). Association for Computing Machinery, New York, NY, USA, 1–10. Doi: https://doi.org/10.1145/800045.801571

Evans R. S. (2016). Electronic Health Records: Then, Now, and in the Future. Yearbook of medical informatics, Suppl 1(Suppl 1), S48–S61. https://doi.org/10.15265/IYS-2016-s006

Eysenbach G. (2001). What is e-health?. Journal of medical Internet research, 3(2), E20. https://doi.org/10.2196/jmir.3.2.e20

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á, & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562. doi:10.1016/j.jbi.2012.12.003

Field, A. P. 2005. Discovering Statistics Using SPSS, Sage Publications Inc.

Fierro, N., & Zapata, C. (2016). Usability Heuristics for Web Banking. Design, User Experience, and Usability: Design Thinking and Methods Lecture Notes in Computer Science, 412–423. DOI: 10.1007/978-3-319-40409-7_39

Furnell, S.M., Jusoh, A. and Katsabas D. (2006), "The challenges of understanding and using security: A survey of end-users, Computers & Security, Vol. 25, No. 1, pp27–35.

Garfinkel, Simson & Richter Lipford, Heather. (2014). Usable Security: History, Themes, and Challenges. Synthesis Lectures on Information Security, Privacy, and Trust. 5. 1-124. 10.2200/S00594ED1V01Y201408SPT011.

Ghauri, P. & Gronhaug, K. 2005. Research Methods in Business Studies, Harlow, FT/Prentice Hall.

Goundar, Sam. (2012). Chapter 3 - Research Methodology and Research Method.

Hausawi Y.M., Allen W.H., Bahr G.S. (2014) Choice-Based Authentication: A Usable-Security Approach. In: Stephanidis C., Antona M. (eds) Universal Access in Human-Computer Interaction. Design and Development Methods for Universal Access. UAHCI 2014. Lecture Notes in Computer Science, vol 8513. Springer, Cham.

Hiranandani, Vanmala. (2011). Privacy and security in the digital age: Contemporary challenges and future directions. The International Journal of Human Rights. 15. 1091-1106. 10.1080/13642987.2010.493360.

Hof, Hans-Joachim. (2012). User-Centric IT Security - How to Design Usable Security Mechanisms.

Hof, Hans-Joachim. (2013). Towards Enhanced Usability of IT Security Mechanisms-How to Design Usable IT Security Mechanisms Using the Example of Email Encryption. International Journal on Advances in Security. 6.

Hof, Hans-Joachim. (2015). User-Centric IT Security - How to Design Usable Security Mechanisms. https://arxiv.org/abs/1506.07167

Holvast J. (2009) History of Privacy. In: Matyáš V., Fischer-Hübner S., Cvrček D., Švenda P. (eds) The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology, vol 298. Springer, Berlin, Heidelberg Institute of Medicine (US) Committee on Regional Health Data Networks; Donaldson MS, Lohr KN, editors. Health Data in the Information Age: Use, Disclosure, and Privacy. Washington (DC): National Academies Press (US); 1994. 4, Confidentiality and Privacy of Personal Data. Available from: https://www.ncbi.nlm.nih.gov/books/NBK236546/

Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Nass SJ, Levit LA, Gostin LO, editors. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington (DC): National Academies Press (US); 2009. 2, The Value and Importance

of Health Information Privacy. Available from: https://www.ncbi.nlm.nih.gov/books/NBK9579/

ISO-9241-11. (2018). Ergonomic of Human-system interaction - Part 11:Usabililty: Definitions and concepts. ISO 9241-11:2018.

ISO/IEC 27000:2009 (E). (2009). Information technology – Security techniques – Information security management systems - Overview and vocabulary. ISO/IEC.

ISO 27799:2008(en). (2008). Health informatics - Information security management in health using ISO/IEC 27002

ISO 27799:2016(en). (2016). Health informatics - Information security management in health using ISO/IEC 27002

Jagadeesh, G., Balakumar, P., & Inamdar, M. (2013). The Critical Steps for Successful Research: The Research Proposal and Scientific Writing. Journal of Pharmacology and Pharmacotherapeutics, 4(2), 130. Doi: 10.4103/0976-500x.110895

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. doi:10.1016/j.jcss.2014.02.005

J. K. Liu, K. Liang, W. Susilo, J. Liu and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," in IEEE Transactions on Computers, vol. 65, no. 6, pp. 1992-2004, 1 June 2016, doi: 10.1109/TC.2015.2462840.

J.Nielsen. (2012). Usability 101: Introduction to Usability. Retrieved from http://www.nngroup.com/articles/usability-101-introduction-to-usability/

John Smith, (2010): "Web Page Design: Heuristic Evaluation vs. User Testing".

JSI (2018), Ethiopia Embarks on Standardizing Its Electronic Health Management Information System, Aavalable online https://thepump.jsi.com/ethiopia-embarks-on-standardizing-its-electronic-health-management-information-system/

Kabir, Syed Muhammad. (2016). Methods of Data Collection.

Kainda, R., Fléchais, I., & Roscoe, A. (2010). Security and Usability: Analysis and Evaluation. 2010 International Conference on Availability, Reliability and Security. DOI: 10.1109/ares.2010.77

Kiennert, C., Bouzefrane, S., & Thoniel, P. (2015). Authentication Systems. Digital Identity Management, 95–135. Doi: 10.1016/b978-1-78548-004-1.50003-1

Kirlappos, I., & Sasse, M. A. (2014). What Usable Security Really Means: Trusting and Engaging Users. Lecture Notes in Computer Science Human Aspects of Information Security, Privacy, and Trust, 69-78. Doi: 10.1007/978-3-319-07620-1_7

Kotzé, Paula & Adebesin, Funmi & Greunen, Darelle & Foster, Rosemary. (2013). Barriers and Challenges to the Adoption of E-Health Standards in Africa.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of medical systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Kulkarni, R. (2018). Mitigating Security Issues While Improving Usability. (Electronic Thesis or Dissertation). Retrieved from https://etd.ohiolink.edu/

Kurtinaityte, L. (2007). E-Health – The Usage of ICT Developing Health Care System : Multiple-Case Study of European Coutries Denmark and Lithuania (Dissertation). Högskolan i Halmstad/Sektionen för Ekonomi och Teknik (SET). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-779

Lampson, B. (2009). Privacy and Security, Usable security. Communications of the ACM, 52(11), 25-27. doi:10.1145/1592761.1592773

Liska, A. (2015). Fusing internal and external intelligence. Building an Intelligence-Led Security Program, 123-137. doi:10.1016/b978-0-12-802145-3.00007-7

Lynda Smith (2019). Fordney's Medical Insurance - E-Book - Ch2 Privacy, Security. And HIPPA. Page 31

Mairiza, Dewi & Zowghi, Didar & Nurmuliani, Nur. (2010). An investigation into the notion of non-functional requirements. Proceedings of the ACM Symposium on Applied Computing. 311-317. 10.1145/1774088.1774153.

Marghescu, D. (2008). Usability Evaluation of Information Systems: A Review of Five International Standards. Information Systems Development, 131-142. Doi:10.1007/978-0-387-68772-8_11

Mendoza-González, R. V., Martin, M. C., & Rodríguez-Martínez, L. undefined. (2011). Identifying the Essential Design Requirements for Usable E-Health Communities in Mobile Devices. E-Health Communities and Online Self-Help Groups, 225–244. Doi: 10.4018/978-1-60960-866-8.ch014

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147, 424-428. doi:10.1016/j.sbspro.2014.07.133

Mills, A. J., Durepos, G., & Wiebe, E. (2010). Encyclopedia of case study research (Vols. 1-0). Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412957397

Moore, W., & Frye, S. (2019). Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules. Journal of Nuclear Medicine Technology, 47(4), 269-272. doi:10.2967/jnmt.119.227819

Moser, C. A. & Kalton, G. 1989. Survey Methods In Social Investigation, Aldershot, Gower.

Najmeh Ghasemifard, Mahboubeh Shamsi, Abol Reza Rasouli Kenar & Vahid Ahmadi (2015): A New View at Usability Test Methods of Interfaces for Human Computer Interaction Volume 15 Issue 1 Version 1.0 Year 2015 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

National Academy of Engineering (US) and Institute of Medicine (US) Committee on Engineering and the Health Care System; Reid PP, Compton WD, Grossman JH, et al., editors. Building a Better Delivery System: A New Engineering/Health Care Partnership. Washington (DC): National Academies Press (US); (2005). 4, Information and Communications Systems: The Backbone of the Health Care Delivery System. Available from: https://www.ncbi.nlm.nih.gov/books/NBK22862/

National Research Council. (1991). Computers at Risk: Safe Computing in the Information Age. Washington, DC: The National Academies Press. https://doi.org/10.17226/1581.

Nielsen, J. and Molich, R (1990): Heuristic Evaluation of User Interfaces.In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Empowering People (Seattle, Washington, United States, April 01 - 05, 1990). J. C. Chew and J. Whiteside, Eds. CHI '90. ACM Press, New York, NY, 249-256.Retrieved on 10/10/05, from ACM Portal.

Nielsen, J. (1994). How to Conduct a Heuristic Evaluation. Retrieved from https://nngroup.com/articles/ten-usability-heuristics/

Nielsen, J. (1994). “Usability Inspection Methods.” Conference Companion on Human Factors in Computing Systems - CHI 94, 1994, DOI:10.1145/259963.260531.

Nielsen, J. (1994). 10 Usability Heuristics for User Interface Design. Retrieved from https://nngroup.com/articles/ten-usability-heuristics/

Nielsen, J. (1995). “Usability Inspection Methods.” Conference Companion on Human Factors in Computing Systems - CHI 95, 1995, DOI:10.1145/223355.223730.

Nielsen, J. (2001). Error-Message-Guidelines. Retrieved from https://www.nngroup.com/articles/error-message-guidelines/

Nielsen, J. (2001). Usability Metrics. Retrieved from https://nngroup.com/articles/ Usability Metrics/

Nielsen, J. (2005a), “Useit.com: Heuristic evaluation”, http://www.useit.com/paper/heuristic/

Nwokedi, Ugochi & Amunga, Beverly & Bashari Rad, Babak. (2016). Usability and Security in User Interface Design: A Systematic Literature Review. International Journal of Information Technology and Computer Science. 8. 72-80. 10.5815/ijitcs.2016.05.08.

Patton M. (2002) Qualitative Research and Evaluation Methods. Thousand Oaks (CA): Sage Publications Ltd.

Perrin, C. (2008, June 30). The CIA Triad. Retrieved from https://www.techrepublic.com/blog/it-security/the-cia-triad/

P. E. Idoga, M. Agoyi, E. Y. Coker-Farrell and O. L. Ekeoma, (2016). "Review of security issues in e-Healthcare and solutions," 2016 HONET-ICT, Nicosia, 2016, pp. 118-121, Doi: 10.1109/HONET.2016.7753433.

Pierotti D, Xerox Corporation (2005) “Heuristic evaluation—a system checklist,” Tech. Rep., Xerox Corporation, Society for Technical Communication

Pope, C. (2000). Qualitative Research in Health Care: Analysing Qualitative Data. Bmj, 320(7227), 114–116. Doi: 10.1136/Bmj.320.7227.114

Punchoojit, L., & Hongwarittorrn, N. (2017). Usability Studies on Mobile User Interface Design Patterns: A Systematic Literature Review. Advances in Human-Computer Interaction, 2017, 1-22. doi:10.1155/2017/6787504

Raven, M. E. and Flanders, A. (1996): Using contextual inquiry to learn about your audiences. SIGDOC Asterisk Journal of Computer Documentation, vol. 20, no. 1, 1-13.Retrieved on 10/1/05, from ACM Portal

Rieman, J., Franzke, M., and Redmiles, D. (1995): Usability evaluation with the cognitive walkthrough. In Conference Companion on Human Factors in Computing Systems. I. Katz, R. Mack, and L. Marks, Eds. CHI '95. ACM Press, New York, NY, 387-388.Retrieved on 9/30/05, from ACM Portal.

Riihiaho, Sirpa. (2001). Experiences with Usability Evaluation Methods.

Rosenbaum, S., Cockton, G., Coyne, K., Muller, M., and Rauch, T. (2002): Focus groups in HCI: wealth of information or waste of resources? In CHI '02 Extended Abstracts on Human Factors in Computing Systems (Minneapolis, Minnesota, USA, April 20 - 25,

2002). CHI '02. ACM Press, New York, NY, 702-703.Retrieved on 11/11/05, from ACM Portal

Ross, J., Stevenson, F., Lau, R. et al. (2016) Factors that influence the implementation of e-health: a systematic review of systematic reviews (an update). Implementation Sci 11, 146 (2016). https://doi.org/10.1186/s13012-016-0510-7

Sahama, Tony, et al. (2013) "Security and Privacy in EHealth: Is It Possible?" 2013 IEEE 15th International Conference on e-Health Networking, Applications, and Services (Healthcom 2013), 2013, DOI:10.1109/healthcom.2013.6720676.

Sandhu, R., & Samarati, P. (1994). Access control: Principle and practice. *IEEE Communications Magazine, 32*(9), 40-48. doi:10.1109/35.312842

Sandhu, R., Hadley, J., Lovaas, S., & Takacs, N. (2015). Identification and Authentication. *Computer Security Handbook*. doi:10.1002/9781118851678.ch28

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). BT Technology Journal, 19(3), 122-131.

Sasse, MA; Flechais, I; (2005) Usable Security: Why Do We Need It? How Do We Get It? In: Cranor, LF and Garfinkel, S, (eds.) Security and Usability: Designing secure systems that people can use. (13 - 30). O'Reilly: Sebastopol, US.

Scholl, Margit. (2018). Information Security Awareness in Public Administrations.

Security Rule Compliance Checklist. (2014). The Practical Guide to HIPAA Privacy and Security Compliance, Second Edition, 257-262. Doi:10.1201/b17548-20

Sittig, D. F., Belmont, E., & Singh, H. (2018). Improving the safety of health information technology requires shared responsibility: It is time we all step up. Healthcare, 6(1), 7-12. doi:10.1016/j.hjdsi.2017.06.004

Srivastava, S., Pant, M., Abraham, A., & Agrawal, N. (2015). The Technological Growth in eHealth Services. Computational and mathematical methods in medicine, 2015, 894171. https://doi.org/10.1155/2015/894171

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems:. Doi:10.6028/nist.sp.800-30. Doi:10.1023/a:1011902718709

Straub, T., & Baier, H. (2004). A framework for evaluating the usability and the utility of pki-enabled applications. In EuroPKI 2004, Proceedings of the 1st European PKI Workshop, 112–125

Sulaiman, Rossilawati & Sharma, D. & Ma, Wanli & Tran, Dat. (2008). A Security Architecture for e-Health Services. International Conference on Advanced Communication Technology, ICACT. 2. 999 - 1004. 10.1109/ICACT.2008.4493935.

Suter, W. N. (2012). Qualitative Data, Analysis, and Design. In Suter, W. N. Introduction To Educational Research: A Critical Thinking Approach (Pp. 342-386). Thousand Oaks, CA: SAGE Publications, Inc. Doi: 10.4135/9781483384443

Sutton, J., & Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. The Canadian Journal of Hospital Pharmacy, 68(3). Doi: 10.4212/Cjhp.V68i3.1456

Tognazzini B (2003) First-principles of interaction design: Interaction Design Solutions for the Real World. http://www.asktog.com/

USAID (2019), USAID Invests in Digital Solutions to Modernize Ethiopia Health System, Extracted from https://www.usaid.gov/ethiopia/press-releases/usaid-invests-digital-solutions-modernize-ethiopia-health

U.S. Department of Education (2003). National Center for Education Statistics. National Forum on Education Statistics. Weaving a Secure Web Around Education: A Guide to Technology Standards and Security, NCES 2003-381. Washington, DC: 2003.

Valverde, Raul. (2011). Principles of Human Computer Interaction Design.

Vance, R. J. (2006). Employee engagement and commitment: A guide to understanding, measuring and increasing engagement in your organization. Alexandria, VA: SHRM Foundation.

Virtual Mentor. (2012);14(9):712-719. Doi: 10.1001/virtualmentor.2012.14.9.stas1-1209

Whitten, A. and Tygar, J.D. (2005), "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", in Cranor, L.F. and Garfinkel, S. (Ed), Security and Usability: Designing Secure Systems That People Can Use, O' Reilly Media Inc., Sebastopol, CA. ISBN: 0-596-00827-9.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security (4th ed.). Cengage Learning

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security. The Need for Security, Ch .2 p59 .Singapore: Cengage Learning Asia Pte.

Y. Barlette and V. V. Fomin, "Exploring the Suitability of IS Security Management Standards for SMEs," Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, 2008, pp. 308-308, Doi: 10.1109/HICSS.2008.167.

Yee, K.-P. (2002). User Interaction Design for Secure Systems. Information and Communications Security Lecture Notes in Computer Science, 278–290. Doi: 10.1007/3-540-36159-6_24

Yee, Ka-Ping. (2004). Aligning security and usability. Security & Privacy, IEEE. 2. 48 - 55. 10.1109/MSP.2004.64.

Yeratziotis, A., Pottas, D., & Greunen, D. V. (2012). A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. International Journal of Human-Computer Interaction, 28(10), 678–694. Doi: 10.1080/10447318.2011.654202

Yeratziotis, Alexandros, et al. "Recommendations for Usable Security in Online Health Social Networks." 2011 6th International Conference on Pervasive Computing and Applications, 2011, doi:10.1109/icpca.2011.6106508.

Appendix A

Support letter from AAU

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: February 14, 2020
Ref No. SIS/46/2020/2012

To:- Addis Ababa Regional Health Bureau

Subject:- Student Antonyo George

Dear Sir /Madam,

Student Antonyo George (ID.No GSE/2000/09) is graduate student at the School of Information System, Addis Ababa University. He is currently conducting a MSc. Thesis research under the title "Evaluating Usability of Security Mechanisms E-health Application: Cases from Ethiopia".

I would like to thank you in advanced for all the assistance that you would provide to the student.

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

✉: 1176 Email: information_sci_cns@aau.edu.et ☎: +251-(11)-122-91-91

Appendix B

Ethical Clearance

አዲስ አበባ ከተማ አስተዳደር ጤና ቢሮ
City Government of Addis Ababa Health Bureau

Ref.No ________
Date 19/6/2012

TO:

- **Addis Ababa City Adminstraton Health bureau**
  Addis Ababa

Subject: Request to access Facilities to conduct approved research

The letter is to support **Antonyo George** of **"Evaluating Usability of Security Mechanisms of e-health applications: Cases from Ethiopia "** The study proposal was duly reviewed and approved by Addis Ababa Health Bureau IRB, and the principal investigator is informed with a copy of this letter to report any changes in the study procedures and submit an activity progress report to the Ethical Committee as required. Therefore we request the facility and staffs to provide support to the principal investigator.

With Regards

Ethical Clearance Committee

Cc

- Antonyo George
- To Ethical Clearance Committee
  Addis Ababa

Appendix C

Consent form

The overall objective of this checklist is to gather information for the purpose of evaluation of three e-health application usability aspect of security mechanisms. The intention of the interview is not to evaluate or criticize you, so please do not feel pressured to give a specific response and do not feel shy if you do not know the answer to a question. We are/I am not expecting you to give a specific answer; there are no good or bad answers. We/I would like you to answer the questions honestly, telling us/me about what you know, how you feel, and the way you take action on the security mechanisms. Feel free to answer questions at your own pace.

The checklist will take two days for each application evaluation with all the experts. All the information we obtain from you will remain strictly confidential and your name and answers will never be revealed. Participation in this evaluation is voluntary and you may refuse to participate, discontinue at any time, or skip any question you do not want to answer.

Do you agree to participate in this interview?

Name:_____ Sig._____

Any questions before we start?

Appendix D

Security Heuristics Checklist

Security Heuristics	Yes	No	N/A	Comment
1. Visibility—the system should keep users informed about their security status				
1.1 If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?				
1.2 If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?				
1.3 After the user completes a security action, does the feedback indicate that the next group of actions may be started?				
1.4 Is there some form of feedback for every security-related action?				
2. Revocability—the system should allow users to revoke any of their security actions				
2.1 Do security options in menus make obvious whether de-selection is possible?				
2.2 Can users easily reverse their security actions?				
2.3 When prompts imply a necessary security action, are the words in the message consistent with that action?				
2.4 Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?				
2.5 Can users cancel out of security operations in progress?				
2.6 Is there an "undo" function at the level of a single security action or for a complete group of security actions?				
3. Clarity—the system should inform users in advance about the consequences of any security actions				
3.1 Are users prompt to confirm security actions that have drastic, destructive consequences?				
3.2 Are the function keys that can cause the most serious consequences in hard-to-reach positions?				
3.3 Does the system warn users if they are about to make a potentially serious security error?				
3.4 Does the system prevent users from making security errors whenever possible?				

4. Convey Features/Expressiveness—the system should guide users on security in a manner that still gives them freedom of expression				
4.1 Are users' initiators of security actions rather than respondents?				
4.2 Does the system correctly anticipate and prompt for the users' probable next security-related activity?				
4.3 By looking, can the user tell the security state of the system, and the alternatives for security-related actions, if needed?				
4.4 Is there a clear understanding of the systems security capabilities?				
5. Learnability—the system should ensure that security actions are easy to learn and remember				
5.1 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?				
5.2 Does the system provide mapping: that is, are the relationships between security controls and security actions apparent to the user?				
5.3 Are security operations easy to learn and use?				
5.4 Are there security selection defaults?				
5.5 Do GUI menus make obvious which security items are selected?				
5.6 Does the system protect users from making severe errors?				
5.7 Is security-related information presented in a standardized manner?				
6. Aesthetics and Minimalist Design—the system should offer users relevant information relating to their security actions				
6.1 Is only the security information essential to decision making displayed on the screen?				
6.2 Are all security icons in a set visually and conceptually distinct?				
6.3 Are security labels brief, familiar and descriptive?				
6.4 Are security prompts expressed in the affirmative?				
7. Errors—the system should provide users detailed security error messages that they can understand and act upon				
7.1 Are security-related prompts stated constructively, without overt criticism of the user?				
7.2 Do security-related error messages inform the user of the errors severity?				
7.3 Do security-related error messages suggest the cause of the problem?				

7.4 Do security-related error messages indicate what action the user needs to take to correct the error?				
7.5 Are the security-related error messages accurate in their descriptions?				
8. Satisfaction—the system should ensure that users have a good experience when using security and that they are in control				
8.1 Is each individual security setting a member of a family of security options?				
8.2 Has colour been used specifically to draw attention and indicate status changes for security-related actions and information?				
8.3 Do security-related prompts imply that the user is in control?				
9. User Suitability—the system should provide options for users with diverse levels of skill and experience in security				
9.1. If the system supports both novice and expert users, are multiple levels of security error messages detail available?				
9.2 Can users choose between iconic and text display of security information, where appropriate?				
9.3 If the system supports both novice and expert users, are multiple levels of security detail available?				
9.4 Can users easily change the level of security detail?				
9.5 Can users easily change between novice and expert levels?				
9.6 Can users customize security to meet their individual preferences?				
10. User Language—the system should use plain language that users can understand with regards to security				
10.1 Are security actions named consistently across all prompts in the design?				
10.2 Are security objects named consistently across all prompts in the design?				
10.3 Is security information accurate, complete and understandable?				
10.4 Are security questions stated in clear and simple language, where used?				
10.5 Is privacy jargon avoided?				
10.6 Is security jargon avoided?				
11. User Assistance—the system should make security help apparent for users				
11.1 Is there a security help function visible (e.g. a key labeled “Security Help”)?				

11.2 Is the security information provided relevant?				
11.3 Can users easily switch between security help and their work?				
11.4 Do instructions follow the sequence of user security actions?				
11.5 Does the system provide users with updated security educational opportunities, if they desire it?				
12. Identity Signal—the system should have valid certificates and the information should be available on the browser of use				
12.1 Does the system notify the users when they are interacting with non-trustworthy sources (no trustworthy is a source that has no information about its identity)?				
12.2 Is the information displayed in the identity signal derived from validated certificates?				
12.3 Does the identity signal include human-readable information about the certificate subject?				
12.4 Does the identity signal include the Issuer fields' organization attribute to inform the user about the party responsible for that information?				
12.5 Are there privacy indicators informing users about the privacy practices of the system?				
13. Security and Privacy—the system needs to consider integrity, availability, confidentiality, and privacy				
13.1 Are protected areas completely inaccessible?				
13.2 Can protected or confidential areas be accessed with certain passwords?				
13.3 Is it clear that the users give consent regarding the use of their personal information?				
13.4 Is it clearly stated for what purposes users' personal information is used?				
13.5 Does the system grant access to a user based on valid authorization?				
13.6 Can the user update or delete inaccurate personal information?				
13.7 In the case where the user must provide sensitive personal information, does the system state what measures are used to protect this data?				
13.8 Does the system notify users on their access privileges?				
13.9 Does the system initiate a session lock after a period of inactivity or upon user request?				

13.10 Does the system enforce a limit of consecutive invalid access attempts by a user during a period of time?				
13.11 Are notification messages relating to security and privacy displayed to the user before access to the system is granted?				
13.12 Are there controls in place that will assist the user in making sharing/collaboration decisions?				
13.13 Does the system ensure that publically accessible information does not contain nonpublic information?				
13.14 Does the system install required software updates automatically and notify the user about this action?				
13.15 Does the system employ automated tools that provide notification to the user upon discovering discrepancies during integrity verification?				
13.16 Does the system notify the user about the procedure to be followed in the case of duplication or loss of personal information?				
13.17 Does the system employ automated mechanisms to assist in the reporting of security incidents?				
13.18 Does the system notify the user of any information system weaknesses or vulnerabilities associated with reported security incidents?				
13.19 Does the system notify the user about the conduct of backups relating to their personal information?				
13.20 Is there a backup policy that regulates how copies of information should be taken and tested regularly?				-
13.21 Does the system provide awareness and educate the user on how to complete tasks?				
13.22 Does the system enforce minimum password complexity of defined requirements?				
13.23 Does the system encrypt passwords in storage and in transmission?				
13.24 Does the system enforce password minimum and maximum lifetime restrictions?				
13.25 Does the system prohibit password reuse for a defined number of generations?				
13.26 Does the system employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission?				
13.27 Does the system require users to confirm statements indicating that they understand the conditions of access?				

Appendix E

6.5 Data Analysis

	Aggregate of aggregate	OpenEMR Aggregate	DHIS2 Aggregate	SmartCare Aggregate
1. Visibility—the system should keep users informed about their security status				
1.1 If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?	no delay & no progress notification	No delay	online version delay setting changes & no progress information, no significant observable delays	login appear no delay, don't show symbol or progress bar/percentage, process without notification & display final output
1.2 If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?	not clearly specify the error (username/password)	does not clearly specify the error / username or password & error in plain text	no pop-up & no clear, specific error username/password request all again	error notification is visible , unhandled exceptions (sql DB) with out specific details

1.3 After the user completes a security action, does the feedback indicate that the next group of actions may be started?	feedback for none security actions only for confirmation	feedback indicated	no security action completion feedback	don't show next step , only confirmation to continue & exit
1.4 Is there some form of feedback for every security-related action?	error & confirmation messages	error and confirmation msg	error feedback invalid username & password	few feedback with some general information (region, wereda, clinic site, site code)
2. Revocability—the system should allow users to revoke any of their security actions				
2.1 Do security options in menus make obvious whether de-selection is possible?	allows deselection , checkbox & group selection with no visible notification to revert	check box & group selection , reverse , enforce	entry error highlight fields with red & request corrections, shows changes hasn't be made	no visible notification to revert, & allows de-selection or reverting action but in general de-selection

				security mgt if user don't want it
2.2 Can users easily reverse their security actions?	no undo button to revert	no single button to reverse & repeat the steps again	not allowed to save errors possible if logically correct for modification & security action can't be reversed	follow same procedure to make change , don't have undo button to revert
2.3 When prompts imply a necessary security action, are the words in the message consistent with that action?	describe the action in consistent	best describe the action & administrator do the security features	security action message is consistent	message are consistent with action
2.4 Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?	similar keys with same action	same action	same keys same action, similar across	keys are comply with action & similar key are same
2.5 Can users cancel out of security	progress can't be stopped or terminated	severity action in progress can't be stopped	no instance for terminate	small time to be execute & mechanism

operations in progress?			action in progress	to cancel before proceeding but close button don't stop security in progress
2.6 Is there an "undo" function at the level of a single security action or for a complete group of security actions?	no undo button	No undo	no undo	no undo button to revert
3. Clarity—the system should inform users in advance about the consequences of any security actions				
3.1 Are users prompt to confirm security actions that have drastic, destructive consequences?	defined roles with summarize change of sensitive data	no confirmation	defined set Roles & modification of security informs data loss/loss of access	summarize change & show validity issues with sensitive nature, unto user to revise actions

3.2 Are the function keys that can cause the most serious consequences in hard-to-reach positions?	actions are grouped in similar location	similar location & not hard to reach positions	actions are in group & no severe security only display denied access	not hard-to-reach position b/c related function keys are grouped and remind users & graphic key allow mouse, keyboard function pads
3.3 Does the system warn users if they are about to make a potentially serious security error?	no security warning	No security warning messages	doesn't show & recommend to add security warning messages.	notification but not for all actions & no such info weak/strong password usage
3.4 Does the system prevent users from making security errors whenever possible?	disabled by default & no blocking mechanism	No feature to inform & disabled by default	access denied displayed & highlighted to be visible/accessible, prevents security errors. E.g. some security	warnings are not related to security & no blocking mechanism (decrementation / timeout session)

			features are disabled	
4. Convey Features/Expressiveness—the system should guide users on security in a manner that still gives them freedom of expression				
4.1 Are users' initiators of security actions rather than respondents?	users are respondents	Users are respondents & can set some security reminder	users are security initiator & sometime responders	system prompts initiation for security action, also automatically validity check & expect confirmation
4.2 Does the system correctly anticipate and prompt for the users' probable next security-related activity?	not prompting for next security action	User schedules to be notified	not available	not prompting for next action & only one way for security action

4.3 By looking, can the user tell the security state of the system, and the alternatives for security-related actions, if needed?	no description of security state recommended to have in the future	description of security state & recommend this for future	section of system displays a summary of the user account setting the current user settings & feature for future	login ID & Password control box highlighted Blue outline with cursor blinking
4.4 Is there a clear understanding of the systems security capabilities?	labels are self explanatory easy to understand but user don not understand security capability as to technical person	labeled with self-explanatory titles, easy to understand the outcome	descriptive texts , easy to understand selection or modification of the fields result & two way authentications, But the user doesn't understand security capabilities	most of them are not readily/clearly understandable but easy for technical person but it protect the next session
5. Learnability—the system should ensure that security actions are easy to learn and remember				

5.1 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?	similar actions are grouped in sequence	good & similar actions are grouped and sequenced logically with brief explanation	similar actions are grouped into menus with similar nature & sequence	associated title & grouping are available
5.2 Does the system provide mapping: that is, are the relationships between security controls and security actions apparent to the user?	preconfigured by admin	preconfigured by administrator		
5.3 Are security operations easy to learn and use?	easy to learn	simple titles and mapping , easy to learn	labels assigned logically tied to their action & association descriptions easy to learn	limited security option are embedded & easy to master (no vague language, clear & low level)
5.4 Are there security selection defaults?	prefilled default value	prefilled default applicable otherwise not	certain fields default values that can be easily modified eg. Single	login box appears at startup

			factor authentication	
5.5 Do GUI menus make obvious which security items are selected?	well explained with default value		default values, an obvious input considering preceding action entries made by the user	well explained
5.6 Does the system protect users from making severe errors?	trying to guide users before Sevier error happen	poor & accept any	before severe error the system warn user about the consequences & access denied or hidden with role based defined.	change is immediate following yes/no option guides users from error
5.7 Is security-related information presented in a standardized manner?	follows some standard text popup & welcome screen with ID / password	No information about security	presented in text pop-ups	some what it follows standard welcome windows with ID & Password box

6. Aesthetics and Minimalist Design—the system should offer users relevant information relating to their security actions				
6.1 Is only the security information essential to decision making displayed on the screen?	informative messages are displayed	informative messages are displayed & assists the user to make decisions	messages are displayed	knowledge of system to understand displayed information & they are integrated in one interface
6.2 Are all security icons in a set visually and conceptually distinct?	minimal & distinctive security icons	minimal & distinctive.	distinct security action	district symbol & font color used for warnings/actions
6.3 Are security labels brief, familiar and descriptive?	clear & simple		descriptive & simple	clearly stated
6.4 Are security prompts expressed in the affirmative?	explanations are positive		explanation in positive	common Yes, No & Cancel
7. Errors—the system should provide users				

detailed security error messages that they can understand and act upon				
7.1 Are security-related prompts stated constructively, without overt criticism of the user?	constrictive message without criticism	show constrictive message with out criticism	error highlighted in red with detail description & do next action without insulting	Not that much comment
7.2 Do security-related error messages inform the user of the errors severity?	no severity information & recommended feature for future	severity message & good feature for future	descriptive without severity & feature for future	change messages indicated without level of severity
7.3 Do security-related error messages suggest the cause of the problem?	do not suggest	doesn't suggest the cause just display the happening.	don't suggest cause	no option
7.4 Do security-related error messages indicate what action the user needs to take to correct the error?	general & few error indicated & need for fix	general & few error only indicated, need fix.	suggest general indication & measures to correct	open & allows to make errors

7.5 Are the security-related error messages accurate in their descriptions?	only general message with out specific details	general & accurate message, lack specific details	general error with accurate	sometimes & design error eg (type password without username)
8. Satisfaction—the system should ensure that users have a good experience when using security and that they are in control				
8.1 Is each individual security setting a member of a family of security options?	predefined security & access with out hierarchy & no inheritance	predefined Security & Access Control Groups with out hierarchical structure	no parent - child r/s, no inheritance & umbrella options are mapped	no hierarchical, no inheritance security relationship & only admin
8.2 Has color been used specifically to draw attention and indicate status changes for security-related actions and information?	no distinct coloring & recommended feature for future	even though no district coloring good feature for future	highlighted in red & good feature for future	color is used in few security description eg (login :green & close: red)

8.3 Do security-related prompts imply that the user is in control?	no control indicated	no prompt	no observable indications user control over action	
9. User Suitability—the system should provide options for users with diverse levels of skill and experience in security				
9.1. If the system supports both novice and expert users, are multiple levels of security error messages detail available?	predefined security & access on interface with out multiple level, recommended feature for future	predefined Security & Access , doesn't have multiple levels which is good for features in the future & allows any allowed user to access the security features	same message shown, no multiple levels & feature for future	access with one interface & control
9.2 Can users choose between iconic and text display of security information, where appropriate?	no only predefined & recommended feature for future	doesn't have any & good features	need improvement	iconic display is available
9.3 If the system supports both novice	predefined security &	predefined Security &	don't have separate	

and expert users, are multiple levels of security detail available?	access without multiple levels, recommended feature for future	Access , doesn't have multiple levels which is good for features in the future & allows any allowed user to access the security features	feature/module for multiple level	
9.4 Can users easily change the level of security detail?	elevated or admin defined role & recommended feature for future	elevated user first to grant and good for feature for future	admin define role & feature for future	
9.5 Can users easily change between novice and expert levels?	admin defined role & same for all user at same level	defined by the role initially assigned & same for same level users	admin define role & same feature for all level	
9.6 Can users customize security to meet their individual preferences?	admin predefined role & recommended feature for future	predefined Security & Access Control & feature for future	admin define role, modification is allowed once login & feature for future	predefined roles with security levels
10. User Language—the system should use plain language that users can understand				

with regards to security				
10.1 Are security actions named consistently across all prompts in the design?	consistent across	shown consistently across	prompts are consistent across	
10.2 Are security objects named consistently across all prompts in the design?	consistent across	shown consistently across	prompts are consistent across, pop-up splash for some notification & bottom of screen.	
10.3 Is security information accurate, complete and understandable?	accurate & complete	partially fulfilled. eg, before changing the password, the system doesn't tell the minimum requirement & complexity.	accurate & complete to understand	
10.4 Are security questions stated in clear and simple language, where used?	simple to understand	stated in a simple-to-understand fashion	simple to understand & no security question, feature for future	English is used

10.5 Is privacy jargon avoided?	no privacy statement	no privacy statements	no privacy statement	
10.6 Is security jargon avoided?	no jargon	no jargons	no jargon	
11. User Assistance—the system should make security help apparent for users				
11.1 Is there a security help function visible (e.g. a key labeled "Security Help")?	online/offline user manual & recommended feature future	Online/offline user manual is available & feature for future	online help are integrated for general features & need improvement to avail security help option	
11.2 Is the security information provided relevant?	relevant but not sufficient & need improvement	manual is relevant but not sufficient	relevant information are incorporated but not sufficient & need improvement	
11.3 Can users easily switch between security help and their work?	online help open in separate tab easy switch	security help presented online in a separate tab but no security help	online help open in new tab makes it easy to switch	

11.4 Do instructions follow the sequence of user security actions?	follows sequence	sequence of the help text is inline with the security features	security features help follows sequence	
11.5 Does the system provide users with updated security educational opportunities, if they desire it?	user manual & online hyperlink for general explanation sites	doesn't go further than giving explanations	user manual available online with hyperlink for general explanations sites	no education option
12. Identity Signal—the system should have valid certificates and the information should be available on the browser of use				
12.1 Does the system notify the users when they are interacting with non-trustworthy sources (no trustworthy is a source that has no information about its identity)?	admin predefined setting & alerts for none trustworthy source	Admin handle setting that site do not interact with external content & browser displays warning of non-trustworthy sources. .	role predefined source availed , no interaction to external sites & alerts for none trustworthy source	
12.2 Is the information displayed in the				

identity signal derived from validated certificates?				
12.3 Does the identity signal include human-readable information about the certificate subject?	readable	readable information with advise	initial alert is readable	no certification
12.4 Does the identity signal include the Issuer fields' organization attribute to inform the user about the party responsible for that information?	informs	informs	it informs	no warnings
12.5 Are there privacy indicators informing users about the privacy practices of the system?	no indicator for privacy		no indicator for privacy	
13. Security and Privacy—the system needs to consider integrity, availability, confidentiality, and privacy				

13.1 Are protected areas completely inaccessible?	predefined Security & Access with protected fields are hidden, inactive, inaccessible	predefined Security & Access & protected fields are hidden, inactive, inaccessible	no visibility for protected area without privilege	
13.2 Can protected or confidential areas be accessed with certain passwords?	admin setup with password & level of access	backend/confidential areas accessed with passwords	admin setup & backend /confidential area have access password	level of access different for different users
13.3 Is it clear that the users give consent regarding the use of their personal information?	no consent & recommended feature for future	no consent & good to have for future	no consent to use personal information	
13.4 Is it clearly stated for what purposes users' personal information is used?	admin capture it but not tell use & purpose of personal information, recommended feature for future	admin capture personal information	don't tell personal information use & purpose, feature for future	no such informative
13.5 Does the system grant access to a user based on valid authorization?	role based	roles defined for a user	role based	

13.6 Can the user update or delete inaccurate personal information?	only administrator allowed & some apps let user to modify personal information	only administrators are allowed	modify own information	
13.7 In the case where the user must provide sensitive personal information, does the system state what measures are used to protect this data?	no , recommended feature for future		to have for future	
13.8 Does the system notify users on their access privileges?	predefined security & access with successful login summary without access privilege	predefined Security & Access & informative messages, access privileges no notification.	successful login show summary of users with out access privileges	happens when users tries to access some element without privilege
13.9 Does the system initiate a session lock after a period of inactivity or upon user request?	admin setup no timeout , only for DHIS2	admin setup & no lockup timeout auto	time bound session lock out	admin setup session
13.10 Does the system enforce a limit of consecutive	admin setup no limit, only for DHIS2	admin setup & no limit for tiring to login	admin setup & limit for	unlimited attempt

invalid access attempts by a user during a period of time?			consecutive attempts	
13.11 Are notification messages relating to security and privacy displayed to the user before access to the system is granted?	first attempt access			happens when first attempt to access
13.12 Are there controls in place that will assist the user in making sharing/collaboration decisions?				
13.13 Does the system ensure that publically accessible information does not contain nonpublic information?	not available			not available
13.14 Does the system install required software updates automatically and notify the user about this action?	notify update before install in case of SmartCare update are centrally	system notify before the update	update is notify before done	updates are centrally without notification

13.15 Does the system employ automated tools that provide notification to the user upon discovering discrepancies during integrity verification?	validation control & notification		have notification function	validation control
13.16 Does the system notify the user about the procedure to be followed in the case of duplication or loss of personal information?	no procedure	no procedure for loss/duplication of personal information	no procedure & guide loss/duplication of personal information	
13.17 Does the system employ automated mechanisms to assist in the reporting of security incidents?	admin setup	admin can post a security incidents & flaws: website OpenEMR	send mail/SMS if configured & feature for future	
13.18 Does the system notify the user of any information system weaknesses or vulnerabilities associated with				

reported security incidents?				
13.19 Does the system notify the user about the conduct of backups relating to their personal information?	admin setup	admin setup to allow user to do backup	data backup not needed for online system by user (personal information)	
13.20 Is there a backup policy that regulates how copies of information should be taken and tested regularly?	backups are available without policy copies tested	Backups are available & integrated, general backup policy with out copies utilization	backup is available without policy how to test copies	
13.21 Does the system provide awareness and educate the user on how to complete tasks?	user manual is available & recommended feature for future	Users guide manuals available offline/Online & feature for future	user manual is available online, without automation to educate & feature for future	
13.22 Does the system enforce minimum password complexity of defined requirements?	admin setup to enforce them in case of OpenEMR user can't change password	admin setup enforce the system without minimum password requirement,	user defined & enforce minimum requirement , complexity	allows user to decide

		users can't change password		
13.23 Does the system encrypt passwords in storage and in transmission?	encrypted	encrypted in storage	not seen directly & password is encrypted	
13.24 Does the system enforce password minimum and maximum lifetime restrictions?	admin setup & enforce expire date otherwise no restriction	configurable & enforce with no lifetime restriction passwords	admin setup password expire date otherwise no lifetime	
13.25 Does the system prohibit password reuse for a defined number of generations?	admin setup & reuse is unlimited only for DHIS2 not allowed	admin setup user defined & reuse the password unlimited	user defined & not allowed to reuse password	no password history
13.26 Does the system employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission?				
13.27 Does the system require users to confirm statements indicating that they	confirmation for change			enforce confirmation for any change

understand the conditions of access?				

Appendix F

Experts agreement on each criterion

	OpenEMR								DHIS2								SmartCare							
	Exp.1		Exp.2		Exp.3				Exp.1		Exp.2		Exp.3				Exp.1		Exp.2		Exp.3			
Security Heuristic	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply	Comply	Not Comply
SH. 1																								
1.1			X		X		66.7			X		X	X		33.3	66.7				X	X		33.3	33.3
1.2	X		X			X	66.7	33.3	X			X		X		66.7	X		X		X		100.0	
1.3	X			X	X		66.7	33.3	X			X		X	33.3	66.7		X		X		X		100.0
1.4	X		X		X		100.0		X			X	X		66.7	33.3	X			X		X	33.3	66.7
							75.0	**16.7**							**33.3**	**58.3**							**41.7**	**50.0**
SH. 2																								
2.1			X			X	33.3	33.3	X			X		X	33.3	66.7				X		X		66.7
2.2				X		X		66.7	X			X		X	33.3	66.7		X		X		X		100.0
2.3	X		X			X	66.7	33.3	X		X		X		100.0				X		X		66.7	
2.4		X	X		X		66.7	33.3		X	X		X		66.7	33.3			X		X		66.7	
2.5				X		X		66.7		X		X		X		100.0				X		X		66.7
2.6				X		X		66.7	X			X		X	33.3	66.7				X		X		66.7
							27.8	**50.0**							**44.4**	**55.6**							**22.2**	**50.0**
SH. 3																								
3.1	X			X		X	33.3	66.7				X		X		66.7	X		X			X	66.7	33.3
3.2			X		X		66.7			X	X		X		66.7	33.3			X		X		66.7	
3.3	X					X	33.3	33.3		X		X		X		100.0	X		X			X	66.7	33.3
3.4	X			X	X		66.7	33.3		X		X	X		33.3	66.7	X			X		X	33.3	66.7
							50.0	**33.3**							**25.0**	**66.7**							**58.3**	**33.3**
SH. 4																								
4.1		X	X			X	33.3	66.7		X	X		X		66.7	33.3		X	X			X	33.3	66.7
4.2				X		X		66.7				X		X		66.7				X		X		66.7

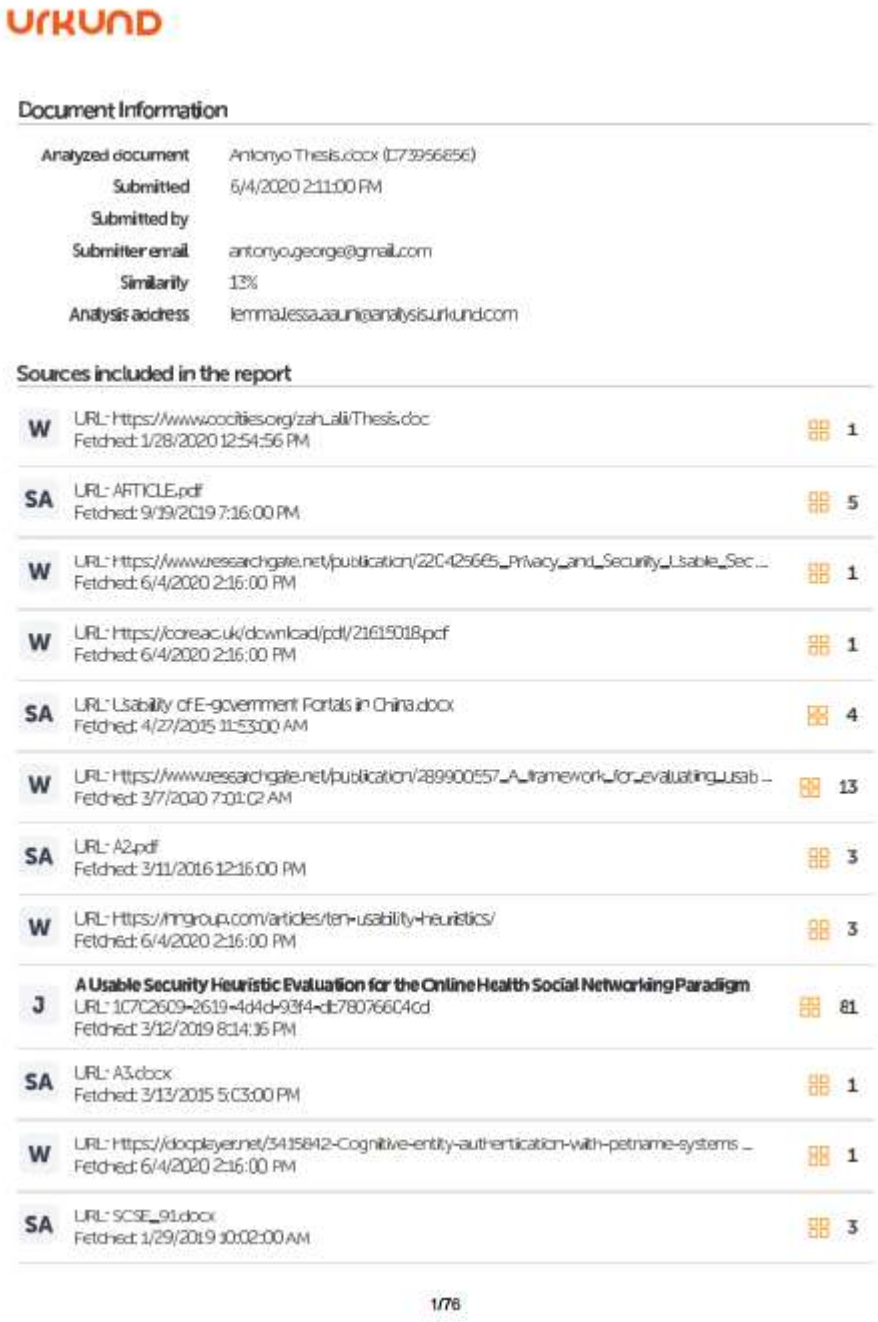
4.3			X			X	33.3	33.3				X		X		66.7		X		X	X		33.3	66.7
4.4	X		X			X	66.7	33.3	X		X			X	66.7	33.3		X		X	X		33.3	66.7
							33.3	**50.0**							**33.3**	**50.0**							**25.0**	**66.7**
SH.5																								
5.1	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
5.2		X	X		X		66.7	33.3	X		X		X		100.0			X	X		X		66.7	33.3
5.3	X		X			X	66.7	33.3	X		X		X		100.0		X		X		X		100.0	
5.4	X		X			X	66.7	33.3	X		X		X		100.0		X		X			X	66.7	33.3
5.5	X		X		X		66.7	33.3	X		X			X	66.7	33.3	X		X		X		100.0	
5.6	X			X		X	33.3	67.7	X		X		X		100.0		X		X			X	66.7	33.3
5.7	X			X		X	33.3	67.7	X		X			X	66.7	33.3	X			X		X	33.3	66.7
							61.9	**38.4**							**90.5**	**9.5**							**76.2**	**23.8**
SH.6																								
6.1	X		X		X		100.0		X		X		X		100.0		X			X		X	33.3	66.7
6.2	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
6.3	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
6.4	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
							100.0	**0.0**							**100.0**	**0.0**							**83.3**	**16.7**
SH.7																								
7.1	X		X		X		100.0		X		X		X		100.0		X		X			X	66.7	33.3
7.2		X		X		X		100.0		X		X		X		100.0	X			X		X	33.3	66.7
7.3	X			X		X	33.3	66.7	X			X		X	33.3	66.7	X			X		X	33.3	66.7
7.4	X		X		X		100.0		X		X		X		100.0		X			X		X	33.3	66.7
7.5	X		X			X	66.7	33.3	X		X		X		100.0			X	X			X	33.3	66.7
							60.0	**40.0**							**66.7**	**33.3**							**40.0**	**60.0**
SH.8																								
8.1	X			X	X		66.7	33.3	X			X	X		66.7	33.3	X			X		X	33.3	66.7
8.2		X		X		X		100.0	X		X			X	66.7	33.3		X		X	X		33.3	66.7
8.3				X		X		66.7		X		X		X		100.0					X		33.3	
							22.2	**66.7**							**44.4**	**55.6**							**33.3**	**44.4**
SH.9																								
9.1				X		X		66.7				X		X		66.7				X		X		66.7

9.2				X		X		66.7				X		X		66.7				X	X		33.3	33.3
9.3				X		X		66.7				X		X		66.7				X		X		66.7
9.4				X		X		66.7				X		X		66.7				X		X		66.7
9.5				X		X		66.7				X		X		66.7				X		X		66.7
9.6		X		X		X		100.0				X		X		66.7				X		X		66.7
							0.0	**72.2**							**0.0**	**66.7**							**5.6**	**61.1**
SH.10																								
10.1	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
10.2	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
10.3	X		X			X	66.7	33.3	X		X		X		100.0		X		X		X		100.0	
10.4	X		X			X	66.7	33.3	X		X			X	66.7	33.3	X		X		X		100.0	
10.5	X				X		66.7		X				X		66.7		X				X		66.7	
10.6	X		X		X		100.0		X				X		66.7		X		X		X		100.0	
							83.3	**11.1**							**83.3**	**5.6**							**94.4**	**0.0**
SH.11																								
11.1	X		X			X	66.7	33.3			X			X	33.3	33.3				X	X		33.3	33.3
11.2	X		X			X	66.7	33.3			X			X	33.3	33.3					X		33.3	
11.3	X		X			X	66.7	33.3			X		X		66.7						X		33.3	
11.4	X		X			X	66.7	33.3			X			X	33.3	33.3						X		33.3
11.5	X			X		X	33.3	66.7	X		X			X	66.7	33.3				X		X		66.7
							60.0	**40.0**							**46.7**	**26.7**							**20.0**	**26.7**
SH.12																								
12.1	X		X		X		100.0						X		33.3					X		X		66.7
12.2	X				X		66.7						X		33.3									
12.3	X		X		X		100.0				X		X		66.7							X		33.3
12.4	X		X		X		100.0						X		33.3					X		X		66.7
12.5		X				X		66.7				X		X		66.7				X		X		66.7
							73.3	**13.3**							**33.3**	**13.3**							**0.0**	**46.7**
SH.13																								
13.1	X		X		X		100.0		X		X		X		100.0		X		X		X		100.0	
13.2		X	X		X		66.7	33.3	X		X		X		100.0			X	X		X		66.7	33.3
13.3		X		X		X		100.0				X		X		66.7		X		X	X		33.3	66.7

13.4		X		X		X		100.0						X		33.3		X		X		X		100.0
13.5	X		X				66.7		X		X			X	66.7	33.3	X		X		X		100.0	
13.6		X		X		X		100.0	X		X		X		100.0			X	X		X		33.3	66.7
13.7		X		X				66.7				X		X		66.7					X		33.3	
13.8		X		X		X		100.0			X			X	33.3	33.3		X		X	X		33.3	66.7
13.9	X			X		X	33.3	66.7			X		X		66.7			X		X		X		100.0
13.1		X		X		X		100.0	X		X		X		100.0			X		X		X		100.0
13.11		X		X		X		100.0		X	X			X	33.3	66.7		X		X	X		33.3	66.7
13.12						X		33.3	X					X	33.3	33.3				X	X		33.3	33.3
13.13						X		33.3		X				X		66.7				X		X		66.7
13.14				X	X		33.3	33.3			X		X		66.7					X	X		33.3	33.3
13.15			X					33.3			X				33.3					X	X		33.3	33.3
13.16	X			X		X	33.3	66.7	X			X		X	33.3	66.7	X			X		X	33.3	66.7
13.17		X		X		X		100.0			X			X	33.3	33.3				X	X		33.3	33.3
13.18		X		X		X		100.0				X		X		66.7				X		X		66.7
13.19	X			X		X	33.3	66.7				X		X		66.7						X		33.3
13.2		X		X		X		100.0				X		X		66.7		X		X				66.7
13.21	X		X			X	66.7	33.3	X			X		X	33.3	66.7	X			X			33.3	33.3
13.22	X			X		X	33.3	66.7	X		X		X		100.0		X			X		X	33.3	66.7
13.23			X		X		66.7		X		X		X		100.0		X			X			33.3	33.3
13.24	X			X		X	33.3	66.7		X	X			X	33.3	66.7		X		X				66.7
13.25		X		X		X		100.0	X		X		X		100.0			X		X		X		100.0
13.26	X					X	33.3	33.3	X						33.3		X			X			33.3	33.3
13.27		X		X		X		100.0				X	X		33.3	33.3	X			X			33.3	33.3
							22.2	**64.2**							**45.7**	**32.1**							**28.4**	**51.9**

Appendix F

Plagiarism Report



URKUND

Document Information

Analyzed document	Antonyo Thesis.docx (D73956656)
Submitted	6/4/2020 2:11:00 PM
Submitted by	
Submitter email	antonyo.george@gmail.com
Similarity	13%
Analysis address	lemmajessa.aauni@analysis.urkund.com

Sources included in the report

W	URL: https://www.coolities.org/zah_ali/Thesis.doc Fetched: 1/28/2020 12:54:56 PM	1
SA	URL: ARTICLE.pdf Fetched: 9/19/2019 7:16:00 PM	5
W	URL: https://www.researchgate.net/publication/220425665_Privacy_and_Security_Usable_Sec ... Fetched: 6/4/2020 2:16:00 PM	1
W	URL: https://core.ac.uk/download/pdf/21615018.pdf Fetched: 6/4/2020 2:16:00 PM	1
SA	URL: Usability of E-government Portals in China.docx Fetched: 4/27/2015 11:53:00 AM	4
W	URL: https://www.researchgate.net/publication/289900557_A_framework_for_evaluating_usab ... Fetched: 3/7/2020 7:01:02 AM	13
SA	URL: A2.pdf Fetched: 3/11/2016 12:16:00 PM	3
W	URL: https://nngroup.com/articles/ten-usability-heuristics/ Fetched: 6/4/2020 2:16:00 PM	3
J	**A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm** URL: 1c7c2609-2619-4d4d-93f4-db78076604cd Fetched: 3/12/2019 8:14:36 PM	81
SA	URL: A3.docx Fetched: 3/13/2015 5:03:00 PM	1
W	URL: https://docplayer.net/3415842-Cognitive-entity-authentication-with-petname-systems ... Fetched: 6/4/2020 2:16:00 PM	1
SA	URL: SCSE_91.docx Fetched: 1/29/2019 10:02:00 AM	3

1/76

SA	URL: Heuristic_Evaluation_Group2.docx Fetched: 2/26/2019 11:50:00 AM	1
SA	URL: Assignment3_Part1-Final report.pdf Fetched: 2/26/2019 11:55:00 AM	2