

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

EHRs at King Fahad Specialist Hospital: An overview of professionals' perspectives on the use of biometric patient identification for privacy and confidentiality, taking into consideration culture and religion

A thesis presented in partial fulfilment of the requirements of the degree of
Master in information science
Massey University
Albany, Auckland
New Zealand

Adel Abdulrahman Khwaji

© A. A. KHWAJI, 2016

Abstract

The Kingdom of Saudi Arabia is focused on expanding use of biometric technologies and it is a matter of time before this expansion includes medical institutions. However there is a lack of research on Electronic Health Records (EHRs) in Saudi Arabian hospitals, especially on the staff views and attitudes in relation to confidentiality, privacy, and security policies in the context of Saudi society, which is governed largely by culture and Islam. This research utilised an online survey tool to ask doctors, managers, and IT professionals, at the King Fahad Specialist Hospital (KFSH) about these aspects and explored if they recommend the classic non-biometric access method over the rather intrusive, yet more advanced, biometric patient identification (BPI) technology. Encouragingly, all the participants recommended BPI methods with the least favoured method being the facial recognition method for Saudi female patients. This study also focused on whether staff believed that religious and cultural issues influence EHR privacy and confidentiality, as the literature showed that in certain cases unauthorised revelation of an EHR could lead to honorary killing of the patient. Implications of this research include the need for comprehensive staff training on being culturally aware, as well as training on EHR security policy, privacy, and confidentiality.

Acknowledgments

I would like to acknowledge and thank my supervisor Dr. Brian Whitworth who assisted me with defining the research problem. He later retired before the completion of the research.

I take this opportunity to express my profound gratitude and deep regards to Dr. Kuda Dube for his exemplary guidance, monitoring, and constant encouragement from the time my supervisor retired until the end of this research.

I would also like to take this opportunity to express a deep sense of gratitude to my brothers Yahya Khawaji, Mohammed Khawaji, Bassam Jawad, Zeiad Masfar and Abdulrahim AlGhamdi for their cordial support, valuable information, and guidance, which helped me in completing this task through various stages.

Lastly, I thank my father Abdulrahman Khawaji, my mother Maryam Khawaji, brothers, sisters, and friends for their constant encouragement without which this project would not be possible.

Table of Contents

Abstract	ii
Acknowledgments	iii
Table of Contents.....	iv
List of Tables	vi
List of Figures.....	vi
Abbreviations	viii
Introduction	1
Research problem	4
2.1 Key Concepts	4
2.2 Research Problem.....	6
2.3 Research Aim.....	7
2.4 Research Objectives	8
2.5 Significance of the Research Problem.....	8
2.6 Expected Research Contributions	9
2.7 Summary	10
Literature Review	12
3.1 Electronic Health Records	12
3.2 The Benefits of EHRs	13
3.3 Limitation to EHRs.....	14
3.4 Background of EHRs in Saudi Arabia.....	15
3.5 EHRs: Confidentiality and Privacy	16
3.5.1 EHR Confidentiality and Privacy in Saudi Arabia.	18
3.6 EHR Security Policy.....	21
3.7 Methods of Accessing EHRs	22
3.7.1 Biometrics.....	22
3.7.2 Different BPI techniques	30
3.7.3 Non-Biometrics.....	37
3.8 Review of the Research Questions Based on Findings of the Literature Review 38	
3.9 Summary and Findings of Literature Review	40
Methodology.....	41
4.1 The Research Design	41
4.1.1 Survey Participants	42

4.1.2 Data Collection	43
4.1.3 Survey Structure.....	45
4.2 Sampling Method	46
4.2.1 Sample Size	47
4.3 Data Analysis	49
4.4 Ethical Considerations	49
4.5 Summary	50
Results	51
5.1 Validity of Results	51
5.2 Survey Results.....	52
5.2.1 Participants' Backgrounds at KFSH (Section A)	52
5.2.2 EHR Current Access Patterns at KFSH (Section B).....	55
5.2.3 Existing access control mechanism at KFSH (Section C)	57
5.2.4 Views/ Recommendations on Biometric Access Control (Section D).....	60
5.2.5 Staff views on risks of EHR Security and Privacy Breaches and policies in the KFSH (Section E).	66
5.2.6 Perception of Staff on the Impact of Religion and Culture on privacy and confidentiality of EHRs (Section F).	71
5.3 Summary of Chapter.....	76
Findings and Discussion	77
6.1 The Background of the Cohort.....	77
6.2 The Perception of EHR Security Among the Respondents in KFSH	78
6.3 Staff Awareness on Data Access Technologies and Policies	80
6.4 Security Concerns and Staff Confidence on the New Technology	81
6.5 The Impact of Saudi Culture and Religion on Biometrics.....	82
6.6 EHR Policy	85
6.7 Unauthorised Revelation of EHRs	86
6.8 The Impact of Culture and Religion on EHR Privacy and Confidentiality .	87
6.9 Recommendations	89
Conclusion, implications and limitations	90
References	97
Appendix A: Covering letter and questionnaire	104
Appendix B: Ethics approval received from MUHEC.....	116

List of Tables

Table 1 Reason for selection.....	43
Table 2 Number of each stratum	48
Table 3 Calculation of the required sample size	49
Table 4 Number respondents and sample size.....	51

List of Figures

Figure 1 Biometric facial recognition technique (All internet security, 2015).	30
Figure 2 Biometric iris scanning technique (Le & Jain, 2009).	31
Figure 3 Finger on sensor device, a scanner (RightPatient, 2015)	32
Figure 4 Fingerprinting: spoofing versus real (Rowe, 2005).	34
Figure 5 Hand palm vein scanning technique (Ruiz-Blondet, 2014).	35
Figure 6 Proximity card (Ultra Electronics, 2015).	37
Figure 7 Survey structure	45
Figure 8 Different professionals at KFSH (Q A1).....	53
Figure 9 Number of Saudi and non-Saudi participants (Q A2).....	53
Figure 10 Length of service/ work experience of participating staff in health care (Q A3).	54
Figure 11 Experiencing using EHRs of KFSH staff (Q A4).....	54
Figure 12 Level of access of different staff to EHRs (QB2).....	56
Figure 13 Overall access to EHRs (QB2).	56
Figure 14 Reason for accessing EHRs by different staff members (Q B3).	57
Figure 15 Method used to access EHRs at KFSH (QC1).	58
Figure 16 Biometric techniques at KFSH (Q C2).	59
Figure 17 Non-biometric techniques used at KFSH (Q C3).	59
Figure 18 Opinion on whether BPI systems are more efficient in providing access security (Q D1: SQ1).	60
Figure 19 Opinion on preferable techniques (Q D1: SQ2).	61
Figure 20 Opinion between BPI systems and paper-based techniques (Q D1: SQ3).....	62
Figure 21 Opinion on whether Saudi culture has an impact on BPI (Q D1: SQ4).....	63
Figure 22 Opinions of Saudi and non-Saudi participants on whether Saudi culture has an impact on BPI (Q D1: SQ4).	63
Figure 23 Opinion on whether religion would have an impact on BPI system usage (Q D1: SQ5).	64
Figure 24 Biometric techniques suitable for Saudi men (Q D2).	64
Figure 25 Biometric techniques suitable for Saudi women (Q D3).	65
Figure 26 Responses of the KFSH staff on whether they received any EHR security policy document (E1).....	67
Figure 27 Opinion of the respondents on whether the policy protects the privacy of EHRs (E2).	67

Figure 28 Opinion of the respondents on whether the policy is efficient in protecting EHR confidentiality (E3).	68
Figure 29 Opinion of the respondents on whether the security procedures are fully understandable to them (QE4: SQ1).	69
Figure 30 Opinion of the respondents on whether EHR data can be revealed to patient's family (QE4: SQ2).	69
Figure 31 Opinion of the respondents on whether EHR data can be revealed to patient's friends (QE4: SQ3).	70
Figure 32 Opinion of the respondents on whether cultural issues have an impact on EHR privacy and confidentiality (QF1: SQ1).	71
Figure 33 Opinion of the respondents on whether religion has an impact on EHR privacy and confidentiality (QF1: SQ2).	72
Figure 34 Opinion of the respondents on whether health staff show responsibility for protecting patients' EHR privacy and confidentiality (QF1: SQ3).	73
Figure 35 Opinion of the respondents on whether Saudi patients are fully committed to cultural issues related to privacy and confidentiality (QF1: SQ4).	73
Figure 36 Opinion of the respondents on whether Saudi patients are fully committed to religious issues related to privacy and confidentiality (QF1: SQ5).	74
Figure 37 Opinion of the respondents on whether revealing Saudi EHRs might expose patients' life to danger (QF1: SQ6).	75
Figure 38 Saudis and non-Saudis opinions (QF1: SQ6).	75

Abbreviations

BPI	Biometric Patient Identification
EHRs	Electronic Health Records
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIPs	Health Information Professionals
HIS	Health Information System
HITECH	Health Information Technology for Economic and Clinical Health
ICTs	Information and Communication Technologies
KFSH	King Fahad Specialist Hospital
MOH	Ministry of Health
MUHEC	Massey University Human Ethics Committee
PHC	Primary Health Care
SANHS	Saudi Arabia's National Health Services

Chapter 1

Introduction

Nowadays, information technology is used everywhere including by banks, government departments and offices, restaurants, and hospitals. Due to such technology, information can be stored and accessed securely, promptly, and efficiently. In healthcare settings, such as hospitals, Electronic Health Records (EHRs) are a very valuable source of information that give clinicians a comprehensive background on the patient's medical history treatments and other relevant details including basic demographic information. In emergency departments, immediate access to patient records is critical and could help to save lives as they assist medical staff with making informed decisions about the course of intervention needed. Information technology and EHRs have revolutionised healthcare and the dawn of the "electronic information age" has changed almost every aspect of healthcare; the effects of electronic information technology can also be seen in different aspects of health care (Schnapp & Michaels, 2012).

In a busy hospital environment, EHRs can be accessed and handled by numerous staff members, which increases the risk of patient records being mishandled or the confidentiality and privacy of the patients and their records being inappropriately breached. In Western countries, medical institutes have established policies and protocols on how staff are to handle patient records, including EHRs. These policies stress the importance of not breaching confidentiality and privacy unless they have authorised consent from the patient and also govern when privacy and confidentiality can be broken and how. Breaches can lead to serious consequences for staff such as disciplinary action or dismissal. In comparison to the Western world where privacy and confidentiality in hospitals is well-researched, it is less clear how privacy and

confidentiality are handled in the Middle East and there seems to be a lack of relevant policies in relation to EHRs.

In developing countries, such as the Kingdom of Saudi Arabia, researches on these issues are scarce; however, Saudi Arabia has a unique culture and is deeply religious. Cultural and religious norms in Saudi Arabia govern many aspects of society including what women are allowed to wear in public and closure of shops during prayer times. Furthermore, segregation between men and women in public places is normal in Saudi Arabia. Understandably, religion and culture in Saudi Arabia also have an impact on privacy and confidentiality of EHRs in hospitals. However, it is unknown if hospital staff, who are mainly non-Saudi citizens, understand this impact.

EHRs are mainly accessed by medical staff in two distinct ways: the first is non-biometric, which usually revolves around the classic password access (but also includes other types that will be discussed in Chapter 3) and is used by many hospitals around the world; the second type is biometric, a more sophisticated authentication system that uses the anatomical features of the medical staff or patients. Arab News (2014) advised that Saudi Arabia was taking the lead to create one of the largest biometric hubs in the world; this could also include medical institutes and hospitals. Given the lack of research on EHR confidentiality, privacy, and policy in the Saudi context, this study is particularly important.

This research will explore the views of three sectors of staff in the King Fahad Specialist Hospital (KFSH), doctors, managers, and IT professionals, on confidentiality, privacy, and security policies in relation to EHRs and the surrounding religious and cultural context with a focus on biometric patient identification (BPI) technology. It will focus on how those staff view the impact that religion and culture may have on EHRs,

as well as their attitudes to breaching confidentiality and privacy, including revealing their contents to family members without prior patient consent. It also asks participants about EHR access technology currently in use at the KFSH hospital and their recommendations around that type of that technology.

Chapter 2

Research problem

The purpose of this chapter is to define the major issues facing the current system of patients EHRs, identify the key challenges, state the aim of the research, provide recommendation on how to achieve the research aim by accomplishing research objectives and, finally, indicate the expected contributions of this research.

2.1 Key Concepts

The key concepts covered in this thesis are as follows:

Electronic Health Records (EHRs): EHRs are a comprehensive computer-based collection of health records of individual patients (Waegemann, 2002, cited in Hoerbst & Ammenwerth, 2010). EHRs consist of, but are not limited to, information regarding patient demographics, medical history, radiology reports, medical notes (may include diagnosis and prognosis), and test lab results (Bickford & Hunter, 2006). EHRs are expansive, enduring, and include medical information that can be accessed and updated by different medical professionals, for example, doctors, nurses, physiotherapists, etc. (Smith & Bakalar, 2006, cited in Hoerbst & Ammenwerth, 2010). EHRs ensure easy access to patient data and automate the process, in the sense that information is always available anytime, anywhere.

Biometrics/Biometric Patient Identification (BPI): biometric technology is used to uniquely identify an individual through the characteristics of the human body, such as fingerprint, face, voice, or DNA recognition, to gain access to, for example, medical records (Krawczyk & Jain, 2005). In particular, BPI uses the characteristics of patients to identify them. This research will ask the participants if biometric technology is being

used at the KFSH and will explore five BPI technologies that are commonly used: facial recognition; iris scanning; fingerprints; voice recognition; and hand-palm veins. It will ask which technologies the participants recommend to use with patients.

Non-Biometric: non-biometric tools refer to access methods that do not involve characteristics of the human body to access EHRs such as, PIN, access card, and password. This research will identify either BPI or non-biometrics as a recommended access mechanism, and if Saudi culture and the religion of Islam have an impact on BPI.

EHR Policy Document: an information security strategy document provided by health provider management to its staff (Aldajani, 2012). Strict policies regarding access to EHRs at the KFSH will help protect patient rights. This research will ask if staff at the KFSH were provided with an EHR policy document.

Confidentiality: “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” (McCallister, Grance, & Scarfone, 2010, p. 7). In other words, it is the process taken to ensure that EHRs are safe and secure from public viewing and are only disclosed to authorised individuals.

Privacy: the right of an individual to restrict access to their personal information (Warren & Brandeis, 1890). In EHR settings, privacy can be described as the rights of patients for their EHRs to be kept away from public view (Haas, Wohlgemuth, Echizen, Sonehara, & Müller, 2011).

Culture: “The integrated pattern of human behaviour that includes thoughts, communication, actions, customs, beliefs, values and institutions of a racial, ethnic, religious or social group” (U.S. Department of Health and Human Services, 2001, p. 4).

The day-to-day lives of Saudi people are strongly influenced by their culture; this aspect must be thoroughly considered when selecting the BPI technique for authentication of patients.

Religion (Islam): Oxford Dictionary (2015) explained Islam in the following way:

“Founded in the Arabian peninsula in the 7th century AD, Islam is now the professed faith of more than a billion people worldwide, particularly in North Africa, the Middle East, and parts of Asia. The ritual observances and moral code of Islam were said to have been given to Muhammad as a series of revelations, which were codified in the Koran. Islam is regarded by its adherents as the last of the revealed religions, and Muhammad is seen as the last of the prophets, building on and perfecting the examples and teachings of Abraham, Moses, and Jesus” (p. 1).

2.2 Research Problem

Religion and culture in Saudi Arabia have a substantial and unique impact on the day to day life style of Saudi people. Confidentiality and privacy are very sensitive areas for Saudi patients and breaches of their EHR confidentiality and privacy have led to negative consequences over the years. There are even instances where people have lost their lives because their private information was misused, intentionally or unintentionally, by health staff that had access to patient’s records (this will be explained in Chapter 3). That is why it is very important to explore the opinions of professionals working in hospitals about confidentiality and privacy to assist hospital management with making any necessary changes. It is also important to understand staff opinions on the impact of culture and religion on privacy and confidentiality matters relevant to EHRs, as many of them could be non-Saudi residents who may be unfamiliar with the religious and cultural protocols and norms of Saudi Arabia.

As will be discussed in greater detail in Chapter 3, biometric technology, especially BPI, is quite a revolutionary EHR access technique. Biometrics are gaining increasing popularity internationally and, to some degree, in Saudi Arabia, as the Saudi Arabian government has been placing great emphasis on improving the status of EHR in the country. Biometric technology is well known for its superiority in protecting the confidentiality and privacy of patients' records (Zuniga, Win, & Susilo, 2010). However it is unknown if such technology would be acceptable and whether there would be cultural and religious barriers to the potential roll out of the technology in Saudi hospitals given the intrusive nature of the technology. Needless to say, the success of any technology relies heavily on how acceptable that technology is by the people who use it; especially, when that technology comes in different forms or phases, such as biometric technology.

2.3 Research Aim

The aim of this research was to explore how acceptable BPI technology would be if introduced in Saudi Arabian hospitals, taking into consideration culture and religion. This was done through surveying the opinions of three sectors of staff at the KFSH (doctors, managers, and IT professionals) on different aspects related to EHRs, including two major aspects as follows. Firstly, whether or not the BPI technologies would be more recommended than non-biometric technologies and what BPI types would be recommended, including an exploration of different biometric types. Secondly, this research attempted to discover the views and attitudes of those staff on confidentiality, privacy, and policies on EHR (if any). This will be explored in relation to the Saudi religious and cultural context.

2.4 Research Objectives

The research aims can be achieved by accomplishing the following objectives:

1. Establishing whether participants recommend non-biometric mechanism or Biometric Patient Identification mechanism (BPI) to access Electronic Health Records (EHRs) and which subtypes of those two they recommend.
2. Analysing participants' views of which type(s) of BPI mechanism they recommend (if any) for both Saudi males and females patients: fingerprints; face recognition; iris recognition; voice pattern and/or hand-palm veins.
3. Determining participants' level of awareness and commitment to EHR privacy, confidentiality and policy (if any policy exists) in the Saudi Arabian cultural and religious context.

2.5 Significance of the Research Problem

The use of EHR systems is increasing worldwide due to the need for robust communication, record keeping, and patient's status reports to be handy and available for all healthcare staff. The challenges faced in Saudi Arabia in relation to the subject matter have emphasised how critical the use of an EHR system is in the country. Unfortunately literature on these matters is very scarce. While it is important to assess the beliefs and opinions of Saudi people on the use of EHR in Saudi hospitals, this would be a difficult task, beyond the scope of this paper due to a number of major obstacles. These include assessing the opinions of Saudi citizens, a number of whom are illiterate; Huebler and Lu (2013) highlighted that in the year 2011, 12.8% of Saudi citizens were illiterate and predicted that illiteracy would only drop to 10.7% by 2015. General illiteracy is usually accompanied by technological illiteracy, which would make the task of assessing the opinions or beliefs of Saudi patients even more difficult.

Another major obstacle is that face to face interviews with patients would be the most appropriate research methodology to employ in order to gain a reasonable understanding of the opinions and views of patients about EHRs in Saudi Arabia. Unfortunately, lack of funds and the requirement to travel to the KSA, which would have been costly, meant this was an impossibility. Furthermore, there is an ethical issue surrounding recruitment of patients as subjects for such a study; recruitment would require the researcher to access patient records, including emails, so the questionnaire could be sent to them. This would breach their privacy and even if an alternative methodology, such as interviewing the patients, was utilised, it would be highly unethical to recruit such subjects, due to being vulnerable patients. In addition the cultural and religious barriers that promote the segregation of women from men would make interviewing female patients almost impossible, and thus affect the results of the study.

Accessing the opinions and beliefs of hospital staff (such as those in the KFSH) about privacy and confidentiality of patients in the Saudi cultural and religious context could prove to be valuable and the data it would reveal could be a steppingstone in designing a study that would overcome the illiteracy barrier, as well as any cultural barriers.

Having a secure, trustworthy system will give patients and staff more faith in the health system in Saudi Arabia leading to better health for people in general. In addition, as staff would be responsible for using and introducing this technology-based system to the public, their attitudes, thoughts, and beliefs about that technology matter.

2.6 Expected Research Contributions

The research will contribute to the understanding of acceptance of BPI technologies, along with EHR confidentiality, privacy, and policy in Saudi hospitals from the

viewpoint of staff and explore the level of trust staff have in the current EHR systems. In light of the current study, it is expected that staff will indicate that they are not confident in the current levels of privacy and confidentiality.

It is expected that participants will recommend the non-biometric technology that is currently being used in the hospital over the more advanced and secure BPI technologies, as the latter is more intrusive and hence may not be religiously and culturally appropriate to utilise.

A third expectation is that the results of this study will indicate that staff show a high degree of diligence and awareness when dealing with EHR confidentiality and privacy.

The research will contribute to understanding some of the challenges facing the implementation of a BPI system in healthcare settings in relation to Saudi culture from the perspective of doctors, managers, and IT professionals.

This research will benefit the health services in Saudi Arabia for optimising the privacy and confidentiality of Saudi patient's records. The study will also highlight the cultural and religious influences that may hinder implementation of robust technological paradigms.

2.7 Summary

EHR privacy and confidentiality are critical matters in Saudi Arabia that require a good understanding of the cultural and religious context of the Kingdom. This research will explore the level of awareness and understanding of participants on EHR confidentiality and privacy, the type of data access technology they recommend to use (BPI or non-biometric), and also gain some understanding about the level of trust of the participants on the current data access methodology they are using. This research aims to highlight

the challenges faced in Saudi Arabia in relation to the current practices in place and how to improve the situation in order to improve general health and build trust in the health system.

Chapter 3

Literature Review

This chapter will provide a thorough description of Electronic Health Records (EHRs), including advantages, limitations and types of the technologies, as well as the status of EHRs in Saudi Arabia. It will explore issues around the privacy and confidentiality of EHRs, both globally and in Saudi Arabia, with a focus on Saudi cultural and religious views on these issues, as well as an overview of EHR security policies. This chapter will also include an analysis of different access methods, which include biometric and non-biometric methods, with a focus on the former, followed by the research hypotheses.

3.1 Electronic Health Records

EHRs are a comprehensive computer-based collection of health records of individual patients (Waegemann, 2002). EHRs consist of, but are not limited to, information regarding patient demographics, medical history, radiology reports, medical notes (may include diagnosis and prognosis), and test lab results (Bickford & Hunter, 2006). EHRs are expansive, enduring, and include medical information that can be accessed and updated by different medical professionals, for example, doctors, nurses, physiotherapists, etc. (Smith & Bakalar, 2006). EHRs ensure easy access to patient data and automate the process, in the sense that information is always available anytime, anywhere. This goes a long way to improve healthcare delivery to patients in a time-sensitive manner. EHRs streamline the communication between healthcare providers and receivers and help build productive relationships between healthcare providers. Given that the records can be accessed anytime, anywhere it creates a platform for bringing about significant improvement in healthcare delivery through aspects such as

better and more agile clinical decision making (Silow-Carroll, Edwards, & Rodin, 2012). Some of the ways through which EHRs can improve healthcare delivery to patients include (Bieber, Richards, & Walker, 2005):

- i. Reduction of errors in medical record keeping.
- ii. Availability of information at all times so that healthcare providers can make time-sensitive decisions and prevent delays in healthcare delivery.
- iii. Reduce duplication of tests and procedures, saving time, resources, and money.

The very essence of EHRs is to improve the efficiency and quality of healthcare delivery and for the healthcare providers, such as doctors and nurses, it serves as the best paradigm to achieve the same. However, it also needs to be noted that benefits of EHRs can only be realised when every player in the healthcare sector carries out duties and responsibilities in the best possible manner. Basically it is a collaborative effort between healthcare providers and patients that involves adaptation and improvement of standard practices, which could lead to further improvement of healthcare delivery.

3.2 The Benefits of EHRs

- i. Streamlined data management and healthcare delivery: With EHRs it becomes much easier for physicians to trace the medical history of their patients. In the event that a patient has been under the care of multiple doctors and has had multiple tests, an EHR makes it much easier for all the relevant information to be accessed, compared to paper-based records. Furthermore, being available online, care providers can always access the data irrespective of their geographical locations. This goes a long way in expediting the process of healthcare delivery in a highly time-sensitive manner (Menachemi & Collum, 2011).

- ii. Easy sharing: EHRs also allow dissemination of information in a smooth manner allowing healthcare providers to collaborate. This can significantly improve the outcome of healthcare procedures and enhance patient satisfaction (Menachemi & Collum, 2011).
- iii. Reduction of error: EHRs significantly reduce data error. This serves as a tremendous benefit for care providers and receivers because it eliminates the chances of losing or misplacing any records. This reduction of error can even go a long way in making a difference between life and death (Menachemi & Collum, 2011).
- iv. Less paperwork (environment friendly): Management of hospitals and healthcare centres involve lots of paperwork in a traditional setting and this translates to rising expenditure, both in terms of money and time. Since EHRs completely eliminate the use of paper, routine record keeping tasks become much easier and more cost-effective. Since the information is digitised there is no need for any large storage spaces and finding information becomes easier (Menachemi & Collum, 2011).

3.3 Limitation to EHRs

Even though EHRs have many advantages, there are also many limitations or disadvantages. For example, there is a huge and ongoing cost associated with the initial setup of EHRs, as well as maintenance and upgrading of the software and the databases and the conversion of paper-based records to electronic ones (Menachemi & Collum, 2011). In private practices of some Western countries, if a medical firm decided to implement EHRs, they may have to increase the cost of health care, which would in turn

disadvantage patients (Zandieh, Yoon-Flannery, Kuperman, Langsam, Hyman, & Kaushal, 2008).

Another disadvantage is that some doctors or clinicians feel challenged by new technology because they are used to utilising the classic paper-based system, and struggle immensely with using EHRs (Waegemann, 2003).

A third limitation relates to information security, as Ozair, Jamshed, Sharma, and Aggarwal (2015) argued, most EHR software is not highly secure, which can lead to breaches of privacy and confidentiality of patient information. This is an important challenge for health organisations to address.

3.4 Background of EHRs in Saudi Arabia

The government of Saudi Arabia offers free public health services through the auspices of the Ministry of Health (MOH) (Almalki, Fitzgerald, & Clark, 2011), which includes most of the public health care institutes and agencies in the country. A private sector and some non-governmental public facilities are also available.

The MOH is the administrator of 59.5 percent of the hospital services in the country, whereas private sector services (where fees are charged) consist of about 21.2 percent of available care (Almalki et al., 2011). Other government agencies cover about 19.3 percent of the health care and hospital services (Almalki et al., 2011). Other government agencies include teaching hospitals, armed and security forces medical services, and the Red Crescent. The Primary Health Care (PHC) centres continue to grow. In 2004, 1,848 PHC centres were open in Saudi Arabia and by 2009 the number had increased by 1,189, to a total of 2,037 PHC centres (Almalki et al., 2011).

Development of electronic health is part of the MOH reform plans for the Saudi health care system (Almalki et al., 2011). Saudi Arabia has 256 hospitals with 49,000 beds in public hospitals and 14,000 beds in the private sector (Mahmoud, 2015). Hospitals that have already integrated EHRs into their daily clinical and administrative routines did so by designing and implementing the systems in the strategic plans of the facilities (Mahmoud, 2015). EHR systems are implemented in the health care of inpatients and outpatients and coordinated services, including prescriptions and tests. The use of EHRs is deemed necessary to meet the goal of building the Saudi Arabian Health Information System (HIS).

In general, hospital staff in Saudi Arabia (including administrative staff, managers, nurses, and physicians) are allowed to freely access EHRs, without any sort of patient consent; some believe that EHRs are the property of the hospital (Aldajani, 2012).

3.5 EHRs: Confidentiality and Privacy

Often confidentiality and privacy are used interchangeably, although they are distinct from each other and have two different meanings. In general, confidentiality can be defined as “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” (McCallister et al., 2010, p. 7). In other words, it is the process taken to assure that EHRs are safe and secure from public viewing and are only disclosed to authorised individuals.

Alternatively, privacy is the right of an individual to restrict access to their personal information (Warren & Brandeis, 1890). So in EHR settings, privacy can be described as the rights of patients for their EHRs to be kept away from public view (Haas et al., 2011) and confidentiality can be defined as “the right of an individual to have personal,

identifiable medical information kept private” (Macintyre & Galvin, 2015, p. 686). The international medical law highlights that every patient should have the right to confidentiality and privacy of their own personal and medical information (Cohen & Ezer, 2013). This entails that access is restricted to individuals who are authorised by the patient to have access to his/her medical record. Medical and personal information should be kept between the patient and the authorised persons, who are usually medical professionals. EHR confidentiality is also usually protected by various codes of ethics, such as the Code of Ethics for Health Information Professionals (HIPs) in Canada, which also includes the right to informed consent (International Medical Informatics Association, 2001).

Simon, Evans, Benjamin, Delano, and Bates (2009) conducted a qualitative study on patients’ attitudes towards Health Information Exchange (HIE) in the US and discovered that consent issues, privacy, and security were the uttermost concerns. These concerns related to breaches of privacy, which can reduce patients’ trust in measures taken to assure privacy and confidentiality, especially if they were massive scale breaches. Lorenzi, Kouroubali, Detmer, and Bloomrosen (2009) argued that EHRs are distributed and located in different parts of health service providers, which makes it easy for anyone to read patient records. The advantages can only be benefited from if there is strong trust in the healthcare system coupled with robust protection of health and patients’ data (Hustinx, 2010). As far as this paper is concerned, such advantages may increase the trust of professionals and patients in EHRs and therefore may make patients more relaxed in terms of who can have access to their EHRs.

Why are Confidentiality and Privacy important?

Confidentiality and privacy are important because they foster trust between patients and medical professionals and breaking patients' rights to privacy and confidentiality would negatively impact this relationship. Therefore, lack of trust may make patients apprehensive and less likely to disclose sensitive information, which could impact on the appropriateness of their care (De Bord, Burke, & Dudzinski, 2013) and would eventually make their EHRs less accurate.

3.5.1 EHR Confidentiality and Privacy in Saudi Arabia.

3.5.1.1 Religious Matters

Islam is the main religion in Saudi Arabia and governs many aspects of the lives of practicing Muslims around the world, including relationships, health, laws, and economics (Vogel, 2000). However the matter of medical confidentiality is largely unaddressed by many Islamic institutions, including the International Islamic Fiqh (Juristic) Academy and the Islamic Fiqh Council in the Muslim World League (Alahmad & Dierickx, 2012). There is little research on confidentiality according to Islam. Potentially, failure to address matters of confidentiality could be a complicating factor in relation to access and authorisation control of EHRs.

In Islam, confidentiality and privacy are based on three Islamic values that highlight its importance (Alahmad & Dierickx, 2012);

- Prohibition against backbiting. Quran warns against backbiting one another (Quran: Dwellings 12, cited in Alahmad & Dierickx, 2012).
- The obligation of Protection of secrets.
- Protection of confidentiality as part of loyalty (to Allah).

Alahmad and Dierickx (2012) surveyed institutional fatwas (plural of fatwa; Arabic word for Islamic views on particular new matters used in the Islamic jurisprudence) on medical confidentiality. The survey covered fatwas from a number of international and regional Islamic juristic councils, such as the Saudi General Presidency of Scholarly Research and Ifta, and compared them with the work of individual Muslim authors. This study also reviewed the Islamic literature on when confidentiality can be justified and broken. Alahmad and Dierickx, (2012) discovered the existence of some fatwas on medical confidentiality but they were not related fully to patient confidentiality. This highlights a lack of relevant research on these matters, especially with regards to when confidentiality could be infringed.

Another issue is that Saudi Arabia's National Health Services (SANHS) does not have any consent procedure (electronic and non-electronic) to, for example, give the right to SANHS staff to manage, access, and transfer patients records or to release information to a third party (breaching patient confidentiality) (Aldajani, 2012). Aldajani attributed this problem to lack of awareness on how serious such a matter is.

3.5.1.2 Cultural Considerations

Culture is defined as “the integrated pattern of human behaviour that includes thoughts, communication, actions, customs, beliefs, values and institutions of a racial, ethnic, religious or social group” (U.S. Department of Health and Human Services, 2001, p. 4). The five areas that have been identified as “areas of dissonance” that need to be addressed are listed below (American Medical Association, 1999):

- Trust
- How to handle physical disabilities appropriately
- Respect of family structure and family identity

- The position of medical professionals in the culture
- Respect for patient's cultural, moral, and social rules

An example of how sensitive such matters are and how culturally diverse the Saudi culture is to Western cultures is explained below:

Three American physicians working in a Saudi hospital realised a young, unmarried woman was pregnant, although she was being treated for a spinal problem. Two of the American doctors, who were culturally sensitive, understood that gender roles were very strict, and if her parents learned of the pregnancy she could be killed for bring dishonour to the family. The third doctor was not sensitive to the Saudi culture and felt guilty about lying to the parents. The third doctor agreed to remain quiet, and together the doctors arranged for the young woman to fly to another country for an abortion. Unfortunately, when the young woman was ready to board the plane, the third doctor decided his ethics required him to explain to the father that his daughter was pregnant. The father did not allow his daughter to board the plane and she was taken home. A few weeks later the third doctor asked the young woman's brother about her, and learned she was killed. The killing of the young woman restored honour to the family (Galanti, 2004).

Globally, researchers have addressed the issues surrounding EHRs from the perspective of their own cultures. Security requirements for confidentiality have nothing to do with how the technology works, but are based on ethical and legal concerns (Wainer, Campos, Salinas, & Sigulem, 2008). For example, Wainer et al. (2008) studied ethical and legal concerns in Brazil. The use of EHRs was discussed from the point of view of privacy, integrity, control, and legal value. The researchers developed principles for the

control of EHRs, and confidentiality for patients and healthcare providers, to address different themes.

Saudi Arabia must address similar challenges for the EHR system in a country that also has a large number of foreigners in the population. Social and religious issues need to be seriously considered during planning and implementation in order to set standards that are suitable for Saudi culture in the healthcare sector.

This research will address whether individuals working in a healthcare setting in Saudi Arabia believe that cultural and religious issues impact on the privacy and confidentiality of EHRs.

3.6 EHR Security Policy

An EHR security policy is a rudimentary component of an information security strategy: a weak EHR security policy reflects weak EHR security, and weak EHR security threatens the privacy and confidentiality of patients. An EHR security policy can be defined as a: “high level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specific subject area” (Peltier, 2004). The main objective of information security is “to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations” (Peltier, 2004).

The key objective of information security is to guide management direction and provide support for information security aligned with business benchmarks and laws and regulations (ISO/IEC, 2005). Aldajani (2012) argued that the goal of information security policy is to preserve the confidentiality, integrity, and availability of information resources. Hone and Eloff (2002) stated that an information security policy

is a very significant document in any given organisation and that it should be written carefully. An information security policy defines the parameters of information or EHR access, such as which information can be accessed and by whom (Jaeger, 2007). There is a lack of information on EHR security policy in Saudi Arabia, which is a serious problem (Aldajani, 2012).

This research will seek to address this gap in the literature through looking at the security policy in place at the KFSH and how this policy is viewed by staff in light of its clarity and protection of patient confidentiality.

3.7 Methods of Accessing EHRs

3.7.1 Biometrics

This section includes a wider explanation of biometric technology in order to better appreciate its significance in the healthcare sector. It will also allow the reader to understand the different paradigms of biometric usage in the healthcare sector. Perrin (2002) described biometric technology as a recognition system that utilises the physical or anatomical features of an individual. Some of the most prominent physical traits or features that are used for recognition by technology are iris, voice, face, fingerprint, hand-palm veins, and even odour (Zuniga et al., 2010). When the physical characteristics of an individual are scanned by the system, the data is collected and archived in a dedicated database. In all the following scans, this archived data is matched with the scanned features and if a success match is made, access is granted (Krawczyk & Jain, 2005). Within the healthcare sector, biometric technologies are being viewed as a means of preventing unauthorised people from using the system, managing access to information systems, and ensuring the security of patient records.

It is necessary to have a reliable system in place to verify the patient identity when physicians access EHRs to order medications or tests. Different organisations, such as passport and border control, banks and insurance companies, are already making good use of the technology to fulfil their requirements but one particular sector that is really witnessing an accelerated adoption is the healthcare sector (Bolle, Connell, Pankanti, Ratha, & Senior, 2013).

The healthcare sector has undergone tremendous developments in the 21st century and one aspect of this is the advent of EHRs. More and more hospitals and healthcare centres are implementing EHRs so that they can bring about significant improvements in healthcare data management and patient care delivery (Boonstra, Versluis, & Vos, 2014). However, as care providers migrate towards digitisation of their records and massive data exchange through health information exchanges, concerns regarding breach in data security are also rapidly gaining prominence (Kwon & Johnson, 2014). The biggest fear is regarding unauthorised data access and, given the volume of sensitive patient data available on the network, the chances of corruption and vulnerabilities are significantly increased.

Furthermore, data integrity is a major concern and requires a balanced and uniform approach across all health information exchange platforms when it comes to matching patient records (Ranade-Kharkar, Pollock, Mann, & Thornton, 2014). It is the responsibility of both the healthcare provider and receiver to securely and accurately enter data into the system, especially when the volume of data being entered into the system is increasing at a phenomenal rate, making the HIE networks extremely complex. In this context, upholding the integrity and privacy of the data ceases to remain the

responsibility of one organisation but becomes the collective effort of all players related to the healthcare industry in general.

Given these concerns, the relevance of biometric technology to the healthcare industry is gaining very rapid prominence in the United States. A major reason behind this is the US Health Insurance Portability and Accountability Act (HIPAA) legislation that has brought into effect very strict requirements to ensure privacy and integrity of patient data (Gostin, Levit, & Nass, 2009). To comply with all the integrity and privacy requirements, healthcare providers are discovering the advancements of the biometric technology for safeguarding data privacy and integrity. According to Gostin et al. (2009), organisational implementation of biometrics can ensure HIPAA compliance by:

- i. Protecting the privacy of patients at all costs
- ii. Providing robust network security features
- iii. Providing state-of-the-art web security
- iv. Providing robust network authentication protocols
- v. Providing secure data archival and access paradigms

Given the potential of biometric technology, it will undoubtedly provide excellent avenues to securely use, store, and share EHRs across different platforms.

Mahnken (2014, p. 8), of BIO-key International, stated that “the password is nearing the end of its useful life and biometric technology increasingly provides an effective alternative”. Biometric technology can be utilised to secure and protect patient’s privacy in shared care contexts by making information network systems more secure (Marohn, 2006). It can also provide a suitable solution for guaranteeing accessibility and security to EHRs (Ramli, Ahmad, Abdollah, & Dutkiewicz, 2013). The level of security is increased by preventing fraudulent access to restricted information, as biometric

technology uses the unique physical features of a person (Zhang, 2013). According to Gates (2007, cited in Zuniga et al., 2010), biometrics allows the elimination of end-user generation of passwords, which has become a main security issue for current information systems. In general, using biometric technology as an access control and authentication method enhances the protection of patient privacy.

3.7.1.1 Applications of Biometric Technology in Healthcare

The U.S federal government stipulated that health records for every American citizen had to be digitised by 2014 (Zuniga et al., 2010). At the moment, biometric technologies are being used to safeguard such digitised data in a manner that satisfies the requirements of the HIPAA act. These days, a patient can receive care from a very wide range of care providers over his lifetime and this involves sharing and dissemination of patient information over the network. State of the art biometric technology ensures that there is no security breach at the stage of data exchange (Zuniga et al., 2010). When it becomes necessary, on the part of the healthcare provider, to carry out biometric scanning on site for authentication to access EHRs, the security of the data is already elevated.

The environment of modern hospitals is very complex and challenging and given such conditions, different biometric techniques might not work as expected. Constant use of different liquids and chemicals and usage of surgical latex gloves often results in the failure of biometric fingerprint scanners to scan features accurately (Spence, 2011). It has also been observed that healthcare workers often find it difficult to remove their gloves to scan their fingers and traditional biometric technologies cannot scan through gloves. To circumvent this problem, many healthcare providers are implementing the

multispectral fingerprint sensors that capture features present under the skin, even when the user is wearing gloves (Spence, 2011).

3.7.1.2 Impact of Biometrics on the Healthcare Sector and Potential Future Applications

It is evident that biometric techniques can significantly improve healthcare data security and streamline data access and sharing. However, within the socio-political context there are different facets that need to be considered while implementing a new technology. Different cultures have different values and practices that would influence the acceptance or rejection of a new practice or paradigm. Religious and cultural beliefs could also dissuade people from adopting biometric techniques because scanning body parts may seem inappropriate and intrusive (Whither Biometrics Committee, 2010). Apart from all the cultural, political, and religious issues, concerns around compromise of sensitive data are always present and might be perceived as a direct threat by those who value their liberty and privacy (Whither Biometrics Committee, 2010). Medico-legal issues concerning impersonation and data theft through unauthorised access could also impact healthcare delivery in a major way and there are even possibilities of erroneous rejection of legitimate profiles that could prevent people from receiving care in a time-sensitive manner (Whither Biometrics Committee, 2010).

In spite of these trade-offs, the adoption of biometric technology in the healthcare sector has been extensive in recent years. The different biometric recognition paradigms can rightly be called the future of patient identification, especially in light of the fact that healthcare providers and agencies from across the globe are working towards improving data security and reducing incidences of data compromise and theft (Trader, 2012). Many healthcare providers today continue to rely on smart cards for insurance claims and digitised bracelets for patient identification. These paradigms are highly susceptible

to compromise and theft and the best alternative to them are state-of-the-art biometric techniques. One such technique is vascular recognition that involves capturing of vein patterns present in the hand of the patient. Such identification paradigms are virtually impossible to duplicate and they hold great promise for the future of patient identification in context of all the threats and concerns of today; particularly breaches to confidentiality of patients and their EHRs (Iacona, 2014).

In order to adhere with patient privacy laws, including the HIPAA, many health institutions in the United States have been utilising biometric technologies to manage privacy and confidentiality of patients and their records and reduce breaches and fraud (Zuniga et al., 2010, Iacona, 2014). Biometric technologies are superior in the protection of privacy of patient data in multiple or share care settings that require a multi-disciplinary team to be involved with the patient (Zuniga et al., 2010). It also significantly decreases the chance of unauthorised access to patient records in comparison with other access methods. Zuniga et al. (2010) argued that the use of biometric technology could be the solution for privacy and confidentiality issues in hospitals as the technology possesses a unique mechanism of identity verification. According to them, it assures that only authorised users can access or alter patient records. Similarly, Okoh and Awad (2015) described biometrics as a fundamental security mechanism that it is more reliable and more capable of protecting patient privacy and confidentiality than traditional methods. Okoh and Awad stated that “biometrics offer a sense of security and convenience both to patients and physicians alike” (p. 93) as they are less likely to be misplaced, lost, forged, or stolen. In contrast, non-biometric methods, such as passwords, are vulnerable to such issues. The patient’s biometric features or information are utilised for authentication to access the patient’s health records. Such an authentication method does not require staff members to

memorise long or sophisticated PINs or passwords that are commonly used in healthcare settings, as the biometric identification of the patient ensures that the correct EHR is accessed (Okoh & Awad, 2015). Furthermore, the traditional authentication method requires a patient to state, for example, their name, age, and address so staff members can access their records; this would not work for unconscious or demented patients.

The unique body encryption provided by biometric technology restricts access to sensitive information as it requires the scanning of a bodily feature, such as face, or eye, that is unique to the patient (Okoh & Awad, 2015).

3.7.1.3 Biometrics in Saudi Arabia

The Saudi Arabian government is initiating different programs that are aimed at promoting the acceptance and adoption of biometric techniques in different government and private organisations (Alhussain & Drew, 2009). Saudi Arabia is also at the forefront of creating one of the largest biometric hubs in the globe that will manage data comprising of eye, face, and fingerprint scans from 30 million individuals (Arab News, 2014).

As already mentioned, the successful adoption and integration of any new technology or paradigm is greatly influenced by the socio-cultural dimensions of a region. In the context of Saudi Arabia, facets such as religion, tribal culture, and rapid urbanisation hold considerable significance (Abdullah, Rogerson, Fairweather, & Prior, 2006). Home to two of the holiest cities in the world, Mecca and Medina, religion in Saudi Arabia is very important. The culture of the people, the different social norms, traditions and patterns of Saudi society are greatly influenced by Muslim values and the acceptance or

rejection of any new technology is largely dependent on whether it fulfils religious obligations (Al-Saggaf & Williamson, 2004).

When the Internet was first introduced in Saudi Arabia as a service, religious and cultural obligations were primarily taken into consideration before its implementation (Al-Saggaf, 2004). Avenues were explored to ensure that offensive material, such as pornography, was properly restricted and Internet filters were in place to block any information that could destabilise the social balance of Saudi Arabia or go against the cultural or religious norms (Al-Saggaf, 2004).

Similarly, when the different avenues of BPI are taken into consideration, the Saudi culture may have an influence with regards to perceiving the level of intrusiveness during scanning of an anatomical feature. Saudi Arabia is a prominent Islamic nation that possesses a strict dress code for women in compliance with a rather rigid version of Sharia law, where women are required to wear a niqab (headscarf) (Aziz, 2011). The face does not have to be covered but in recent years religious hardliners have raised strong objection to this. In essence, all the facial features of a woman are covered and biometric authentication through face scanning will not be possible (Al-Harby, Qahwaji, & Kamala, 2009). The Saudi society is definitely witnessing a massive change, especially after King Abdullah came to power in 2005. Before his death he was able to herald a transformation that witnessed a growing number of women joining the Saudi workforce. However, emancipation of women is still a complicated matter and the situation is further complicated by the clash of opinions between the radical and liberals (Mittestaedt & Shafy, 2015).

3.7.2 Different BPI techniques

3.7.2.1 Facial recognition

This technique involves scanning facial features and attributes for the purpose of determining the identity of an individual. The facial features scanned by the system include size, shape, and position of the eyes, shape and position of the nose, shape of the cheekbones, and the formation of the jaw line (Zhao, Krishnaswamy, Chellappa, Swets, & Weng, 1998). These features are extracted from the images captured by the camera on the device and require the individual to look straight into the camera. At present an updated version is available that allows 3D biometric recognition of facial features. The technique involves the use of a 3D camera that is able to scan the facial features in a much more effective manner (Du, 2013). The technique is ideal for clean environments and is very user friendly but its performance is not very good in low light conditions. Furthermore, different facial expressions, such as a grin or laugh, might significantly bring down the performance of the system (Saini & Rana, 2014). Figure 1, below, illustrates the different elements or features of the human face that are captured by the biometric face recognition technique. Along with the skin texture and facial features, such as moles and warts, the technique also focuses on accessories such as earrings to determine the gender of the individual.

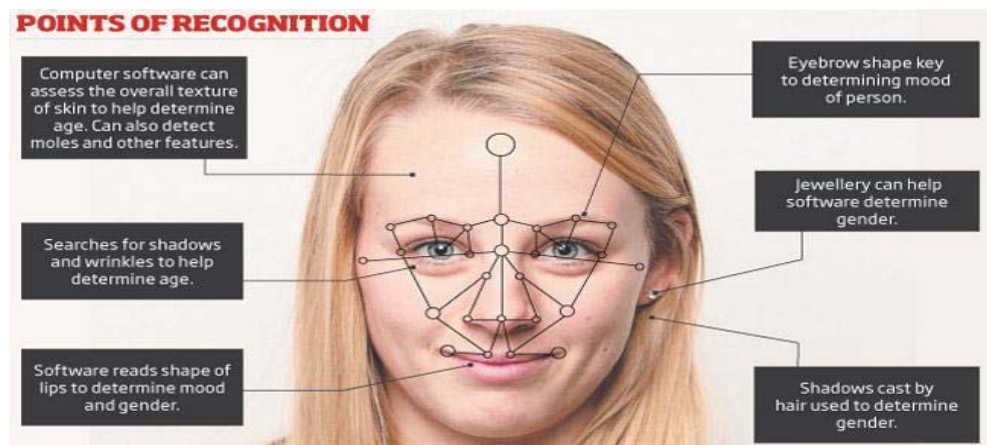


Figure 1 Biometric facial recognition technique (All internet security, 2015).

3.7.2.2 Iris Scanning

This biometric technique is one of the most secure authentication protocols available and it involves different features of the iris such as the rings, spots, and colour (Choudhary, Tiwari, & Singh, 2012). The iris tissue of every individual has a very distinctive texture and they are very different from one another to the extent that even homozygous identical twins have different iris tissue features. The system extracts the impression of the iris and compares it with the one stored in the database. In the event of a positive match, access is granted into the system. The iris scanning technique has very impressive success record and the failure/mismatch rates are very low (Le & Jain, 2009). A major advantage of iris scanning is that the iris features are fully developed by the time a baby is 10 months old and they remain absolutely stable over their lifetime (Klokova, 2010). The technique is not intrusive at all and iris scans can even be carried out from a distance of a few meters. Iris features can be scanned without any issue even if the individual wears contact lenses or glasses and has a processing time of less than two seconds (Le & Jain, 2009).

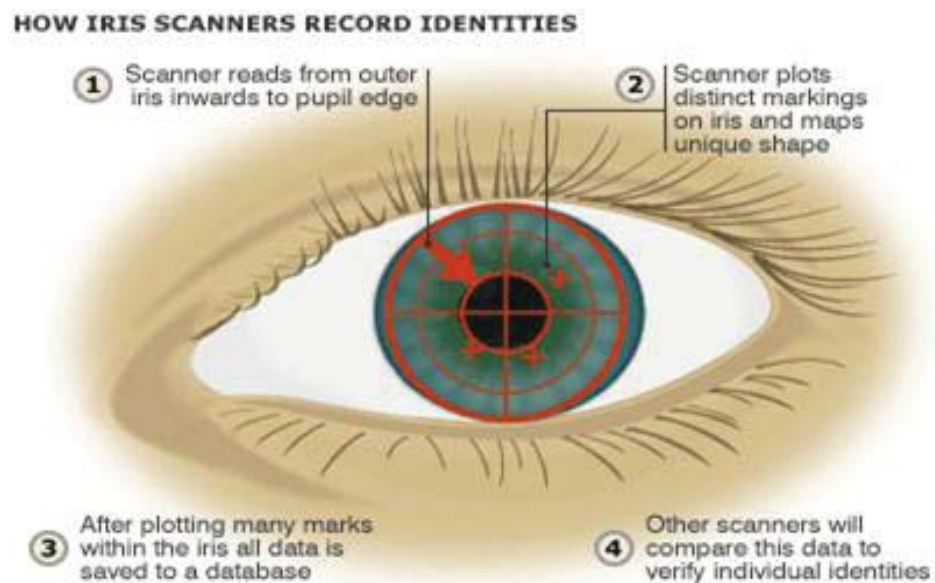


Figure 2 Biometric iris scanning technique (Le & Jain, 2009).

As shown in Figure 2, above, iris scanners capture different features, such as the distance between the iris and the outer pupil ring and other distinctive iris marks, and compare them with the data stored in the database to ascertain the identity of individuals.

3.7.2.3 Fingerprints

A fingerprint is “the pattern of ridges and furrows on the surface of a fingertip, and no two persons have exactly the same arrangement of patterns” (Jaiswal, Bhadauria, & Jadon, 2011, p.28). Fingerprint identification was one of the first biometric technologies introduced, however several limitations have been identified. These include if the data from the sensor is noisy (shows interference), the ability to highlight distinctiveness in a pattern, non-universality, and spoof attacks (Al-Hijaili & Abdulaziz, 2011). Spoof attacks, or spoofing, are the use of a fake fingerprint to allow an intruder into the system (Rowe, Nixon, & Butler, 2008). Fingerprint biometrics requires full contact with the sensor device (see Fig. 3); the best contact is with a finger that is not too wet or too dry. The optics of the device senses the amount of total internal reflectance (TIR), the phenomenon when the boundary between the glass of the device and the air reflects data at specific angles. For that reason the finger must be placed against the plate, but if the finger is too dry or the device is wet or dirty, the scan will not be good. A wet sensor can scan water drops instead of the entire fingerprint and problems may also arise in very dry climates.



Figure 3 Finger on sensor device, a scanner (RightPatient, 2015)

Matsumoto, Matsumoto, Yamada, and Hoshino (2002) explained that some very thin and cheap materials, such as sweets or gummy bears, could be used to make very accurate fingerprints used for identity theft. For that reason biometric techniques that use the sub-dermal as well as the dermal layer of a fingerprint have been developed. Lumidigm (Rowe et al., 2008) devised a spectrographic analysis to compare live human fingers with artificial or fake artefacts. The differences between a prosthetic-finger versus a live finger are depicted by spectrographic analysis below (see Fig. 4). The data is graphed to represent the following characteristics of the signal of the sample, in this case the prosthetic or live finger: the horizontal axis represents time, the vertical axis is the frequency, and the third dimension represents the amplitude by intensity of colour. Another fingerprint strategy, developed by Wang, Hu, and Phillips (2007), is known as the Fingerprint Orientation Model Based on 2-Dimensional Fourier Expansion (FOMFE). The strategy was designed for application to a one-point detection using fingerprint indexing. Fingerprints can be utilised even if part of the fingerprint was “reconstructed” with insufficient information (Ross, Shah, & Jain, 2005).

Despite these issues the future of fingerprints in hospitals looks very promising. Hembroff, Wang and Muftic (2011) have been working on a new technology which they termed Master Patient Identifier (MPI) and uses a combination of fingerprints and PINs. They argued that this combination would significantly improve the confidentiality and privacy of patients and their records.

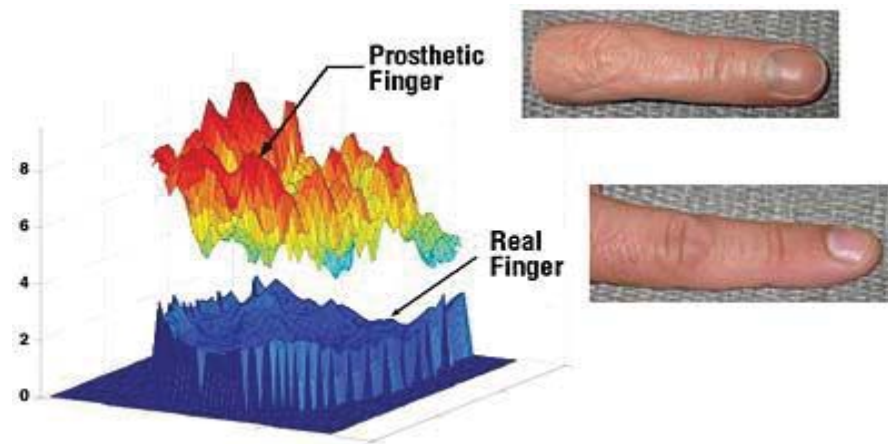


Figure 4 Fingerprinting: spoofing versus real (Rowe, 2005).

3.7.2.4 Voice Recognition

Voice is a “combination of physical and behavioural biometrics” (Jain, Ross, & Pankanti, 2006, p. 127). Voice recognition matches particular voice traits with templates stored in a database to distinguish an individual (Delac & Grgic, 2004). The platform for VoiceVault has the ability to recognise 358,400 bits per second of a speaker (True, 2012). Voiceprints are stored and then when a patient says a very short phrase their voice is compared to the voiceprints. The degree of similarity is measured. At a high enough degree of similarity the user is verified. “The accuracy of this process is exceptional, allowing voice biometrics to even serve as digital signatures for e-prescribing and e-sampling with false accept rates in a statistical model under .01 percent” (True, 2012, para. 11).

A drawback of voice recognition is that it only works well when the user accesses the system in a private location. Voice biometrics work well in a quiet, private environment, but using voice is not reliable in noisy, crowded environments due to inaccuracies from the interference of other sounds (Jaiswal et al., 2011). The advantages of the voice biometric are that the user only needs a few seconds to speak a short phrase, and does not need to carry a card or memorise passwords and PINs. The

low rate of false acceptance rates converts into a one in 10,000 chance that an unauthorised user can enter the system (True, 2012).

3.7.2.5 Hand-Palm Veins

Hand vein geometry is “based on the fact that the vein pattern is distinctive for various individuals” (Bhattacharyya, Ranjan, Farkhod Alisherov, & Choi, 2009, p. 21). The palm veins have been considered as having the same advantages as fingerprinting. At one time the health care sector was interested in this technology, because the hand does not have to touch the reading device, therefore, constant sanitisation of the device is not necessary, unlike with fingerprinting (Mahnken, 2014). The disadvantages include cost, because the large image necessitated by the size of the palm requires larger sized devices, accuracy and difficulties with adapting a secure platform with mobile devices (Mahnken, 2014).

As seen in Figure 5 below, the vein patterns of the hand are captured by the system and the features are unique for every individual. Since the veins on the palm are scanned by infrared light, they appear as dark lines on the scan (Bhattacharyya et al., 2009)



Figure 5 Hand palm vein scanning technique (Ruiz-Blondet, 2014).

A robust BPI system that effectively protects privacy and confidentiality has been utilised successfully in some health settings (Omotosho, Adegbola, Adelakin & Adelakun, 2015). To access EHRs, the system used multimodal BPI (fingerprints and iris of patients) in pre-hospital care. The system improved privacy and confidentiality by restricting the amount of data exposed to professionals or users. The system even works successfully in emergency situations as staff can access necessary or relevant patient data via fingerprints and iris of patients.

Diaz-Palacios, Romo-Aledo, and Chinaei (2013) advocated for the use of the BPI technology of fingerprints (uni-model biometrics) in hospitals with patients. Diaz-Palacios et al. (2013) argued that uni-models have several limitations such as:

- Noise in a sensed data - a scar on the finger or certain sickness symptoms could distort the biometric data.
- Intra-class variations – These happen when incorrect interfacing with sensors such as incorrect facial pose.

The current study will explore the views of staff in KFSH on the use of BPI technologies with patients (uni-models as opposed to multi-models).

Given that the Saudi government is very keen on the implementation of biometric technologies in different fields, governmental and nongovernmental sectors, this research attempts to assess whether staff in KFSH (doctors, managers and IT professionals) recommend BPI systems over non-biometric ones or vice versa. It also attempts to explore their recommendations for different types of biometric technologies; namely, facial recognition, iris scanning, fingerprints, voice recognition, and hand-palm

veins. Gauging the acceptability of biometric technologies in these hospitals could assist in identifying and resolving potential issues.

3.7.3 Non-Biometrics

3.7.3.1 Proximity Card

Authentication from a potential user is necessary to secure systems from hacker attacks. In the USA, health care providers at hospitals and other facilities historically used proximity cards or badges at the entrance door and for access into workstations and computers (Mahnken, 2014). Cards can easily be lost or stolen; all the credentials, identity, and access of the card's owner can be claimed by the holder of the card. An initial cost must be paid when the card system is first installed, and then, costs are incurred for replacement cards, and for updating the cards. Health care workers can move through wards caring for patients using their personal cards with no difficulty, with EHR systems the same ease of use is necessary to meet their expectations. The problem with using a PIN, a card or some other item is that they can be stolen or lost, but with biometrics the authentication cannot be misplaced or taken by a thief (Wang et al., 2007). As seen in Figure 6, below, when the card is placed against the scanner, the data inside it, such as ID, are captured and sent to the reader. In the event of a match, access is granted.



Figure 6 Proximity card (Ultra Electronics, 2015).

3.7.3.2 Tokens: Hard and Soft

A hard token refers to authentication that sends code dedicated hardware; a soft token is when the code is sent to a telephone or to a computer. An advantage of the soft token is flexibility; they can work with mobile applications or with “remote security platforms” (Mahnken, 2014). Tokens are designed for higher security than passwords. Health care, banking, and retail stores use tokens with the matching dedicated device that can receive only the secure authorisation code. The disadvantage of hard and soft token use is the interruptions in workflow that occur when activating the token and receiving the code. The interruption is only a few seconds, but can be an annoyance (Mahnken, 2014).

3.8 Review of the Research Questions Based on Findings of the Literature Review

(a) Hypotheses

The basic hypothesis is that biometric technology and policy are viable, secure, and an efficient way of addressing security and privacy issues in the healthcare sector. In the context of Saudi Arabia, aspects such as culture and religion play a major role in choosing the most ideal patient information security system to be implemented by health care providers. For this reason, the best EHR access paradigm in Saudi Arabia would be the one that would satisfy all technical and cultural dynamics.

Hypothesis 1: Most Saudi health staff believe that religious and cultural issues have a great influence on EHR privacy and confidentiality.

Findings from literature review

The Saudi culture is bound by strict Islamic Sharia law and any breach in EHR data privacy can have very serious repercussions, especially for women who are required to adhere to a very strict dress code; compromise of sensitive information could jeopardise

their lives. For example, medical information about an unmarried pregnant woman revealed by one of her doctors to her father lead to her death, as described previously in this chapter. The responses of staff gathered in the questionnaire will reflect the influence or the impact of Saudi culture and religion on the privacy and confidentiality of EHRs.

Hypothesis 2: Most Saudi health staff (doctors, managers and IT professionals) will recommend non-biometric methods over BPI methods because BPI methods involve scanning of anatomical parts Saudi patients could be considered intrusive and inappropriate as per the norms of the Saudi culture.

Findings from literature review

One of the prominent BPI authentication techniques is face recognition where the system extracts the features of an individual's face. This would require exposure of the face to the system camera but given the strict dress code of Saudi women where the face needs to be covered at all times in public places, it does not look like a practical option as Saudi cultural and or religious influences will impose that most of the Saudi women will not accept face recognition because they must be covered by a veil.

Conclusion

This study focuses on identifying the recommended method of EHR access (BPI or non-biometric) by key health staff at KFSH in Saudi Arabia. It also focuses on finding out the views of those staff on whether they believe that religious and cultural issues influence EHR privacy and confidentiality. Based on the initial reasoning and understanding of the research problem, the hypotheses were generated and the study involved gathering information from key health staff as the basis of this research to answer the research questions.

(b) Research Questions

- I. What are KFSH staff (doctors, managers, IT professionals) views on privacy, and confidentiality of EHRs?
- II. According to KFSH staff, does the religion of Islam and/or the Saudi culture impact on EHR confidentiality and privacy?
- III. Which EHR access mechanism do the KFSH staff recommend: BPI or non-biometric?

3.9 Summary and Findings of Literature Review

In the Saudi healthcare sector, EHRs can significantly streamline patient data management and access. The literature review chapter presented an exhaustive discussion on the EHR technique in general and also elaborated on the advantages of different BPI and non-biometric techniques currently available for secure data access. The focus of the chapter was also on the relevance and significance of BPI and non-biometric paradigms of data access to the Saudi healthcare sector. Given the sensitivity of the patient healthcare data and the socio-political dimensions of Saudi Arabia, selection of the most appropriate BPI technique for Saudi male and female patients is a critical necessity. The literature review highlighted the strengths and weaknesses of the most popular biometric (including BPI) and non-biometric access techniques available today. With every new technology comes its own set of advantages and disadvantages and EHR and BPI is no different. A major concern with EHR, as already mentioned earlier, is the ever present threat of data breach. Patients' EHRs are relatively new in Saudi Arabia health services and progressing very slowly and there is lack of information on EHR security policy and on EHR in general, not to mention BPI.

Chapter 4

Methodology

This chapter consists of eight main sections: the research design where the type of methodology used will be discussed, survey participants (the reasoning for selecting doctors, managers and IT professionals at KFSH), data collection, survey structure, sampling methods, data analysis (how the data will be analysed), and ethical considerations.

4.1 The Research Design

This study uses a cross-sectional survey design to identify the participants' opinions or points of view on several issues related to EHR, while taking into consideration the dominant culture and the religion in Saudi Arabia.

Survey is a well-known quantitative or qualitative methodology that can be defined as an “information-collection method used to describe, compare, or explain individual and societal knowledge, feelings, values, preferences and behaviour” (Fink, 2009, p. 1). Surveys can be divided into two main categories: interviews and questionnaires. The questionnaire category was selected for this research as it is a useful tool for the collection of information from hundreds of people in a short period of time, as described by Fink (2009). From a practical standpoint, questionnaires are easy to use and allow collection of data from a large cohort and also allow quick, timely analyses of the data and prompt comparison and contrast with other study findings.

According to Preece, Rogers, and Sharp (2002), survey questionnaires are excellent for information gathering and are very useful for collecting demographic data as well as data on participants' views, opinions, and preferences. This is important in this study

because knowing some facts about the participants, such as the length of their experience in health care, or with using EHRs, and whether they are Saudi or non-Saudi would be helpful during the analysis stage of this research. Thus, questionnaires were chosen as the methodology for this research.

Web-based questionnaires save time and energy, can help overcome geographical constraints, and are cost efficient. They allow participation of respondents located thousands of miles away and can also increase the response rate (Spitz, Niles & Adler, 2006). Due to the geographical distance between New Zealand and Saudi Arabia, and the limited research funds, a web-based survey was the most appropriate tool to use in this study.

4.1.1 Survey Participants

For this study, the questionnaire was designed to capture the opinions and views on EHR related issues of health staff. The participants were advised that the information they shared in the survey would remain anonymous and that the study in hand was reviewed and approved by the Massey University Ethics Committee (Appendix B). Answers to the survey questions implied participants' consent.

An online questionnaire was selected due to the fact that participants were not available locally (i.e. they lived in Saudi Arabia) and it would be the most efficient method to save time and money.

A research sample is crucial for the research outcomes and credibility of the gathered data. Bryman & Bell (2015) defined a research sample as: "The segment of the population that is selected for investigation" (p. 187). The chosen sample/respondents consisted of managers, doctors, and IT professionals working at KFSH and as their

work titles suggest, they worked in different departments in the hospital. Table 1, below, summarises the reasoning behind selecting those three types of professionals to conduct the survey. The three groups are quite distinct from each other, which could add more strength to the findings.

Table 1 Reason for selection

	Sample	Reasons of selection
1	Managers	<ul style="list-style-type: none"> ▪ Decision makers who would potentially be involved in any implementation of biometric and non-biometric systems in the hospital and would deal with any related issues. ▪ Decision makers who could be involved in levels of access in an EHR, i.e. who should have access to what.
2	Doctors	<ul style="list-style-type: none"> ▪ The primary users of EHRs. ▪ Dealing with biometric or non-biometric system.
3	IT Professionals	<ul style="list-style-type: none"> ▪ Take part of staff training on the system. ▪ Implement, maintain, and deal with any issues related to EHR.

KFSH was chosen for this research as it is one of the largest and well known hospitals in Saudi Arabia which uses EHRs (KFSH, 2015). KFSH employs 635 doctors, 93 managers, and 132 IT professionals; such figures indicate that it recruits large amount of employees (KFSH, 2015). KFSH is located in Dammam; which is one of the largest cities in Saudi Arabia and the capital of the Eastern province (KFSH, 2015).

4.1.2 Data Collection

An online data collection tool known as LimeSurvey was used to gather data due to its convenience and simplicity. Once the online survey was completed and submitted, the

responses were stored automatically in the researcher's (personal) account in LimeSurvey.

Approval to conduct the questionnaire was requested electronically from the management of KFSH and was granted after four weeks (Appendix A). After this, an email was sent to the hospital administration with background information on the research including the purpose of the research and brief background on the researcher. The email, which included the hyperlink of the research, requested that the email get forwarded to doctors, managers, and IT professionals employed by the hospital. Respondents were allowed to submit their surveys by visiting the LimeSurvey website. When the link was selected the first thing that appeared to the participants was the covering letter, which provided information about the background of the researcher and the research topic (Appendix A).

Response prompts in the questionnaire included checkboxes, radio buttons, and Likert scales. The Likert scale was used to measure the views of the doctors, managers, and IT professionals who participated in the survey. Five degrees of agreement and disagreement with statements were used for the Likert scale. In that way respondents were allowed to choose one of five degrees of the accuracy of the statements from their experience. Some of the answers were two branched, yes or no.

The respondents were given two months to respond to the questionnaire. This was deemed ample time to allow as many participants to take part as possible, and hopefully to obtain a representative data or sample size. After one month, a follow up email with the survey hyperlink was sent to administration and requested that the survey to be emailed to the doctors, managers and IT professionals who did not answer the survey as only 72 respondents participated in the survey at that stage.

Once the completed questionnaires were received the responses were properly organised in Excel sheets according to the different sections so that it would be easier to carry out analysis in the later stages.

4.1.3 Survey Structure

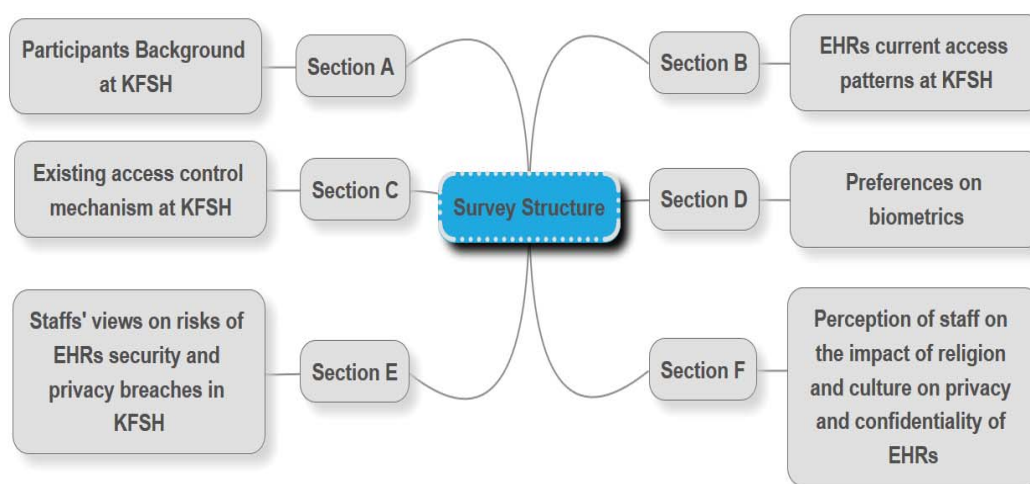


Figure 7 Survey structure

The questionnaire was divided into six different sections: the first section was dedicated to collecting the background information, such as the profession of the respondents, work experience, and familiarity with EHR paradigms.

The second section was all about finding out the current status of EHR usage in the hospital. The questions were designed to determine usage patterns, personnel who had access to EHRs, and the reasons behind accessing electronic patient records.

The third section was dedicated to finding out if the respondents were aware of electronic record access protocols, such as biometric and non-biometric techniques. The respondents were also asked to mention the type of technique currently in use to access electronic patient records and if they believed that biometric techniques were better than non-biometric techniques.

The fourth section scaled the impact of religion and culture on the use of biometric techniques for electronic patient record access. The questions under this section also asked the respondents about the biometric techniques that were suitable for Saudi men and women.

The questions in the fifth section of the questionnaire asked the respondents about their views on security issues surrounding biometric techniques. The respondents were also asked if they were fully aware of the security policies of the KFSH to safeguard patient data and if they are adequate to ensure data privacy and integrity. The section also tried to determine if patient records could be easily revealed to the friends and family of those who have access.

The sixth and final section sought to understand the relevance of culture and religion to Saudi patients in the context of electronic patient data. The section questions also tried to scale the seriousness of any data breach and if such a compromise could be perceived as threatening the life of patients.

The findings were graphically displayed in the form of bar-charts, or pie-charts, for every question. All six sections are defined by a heading statement. The questionnaire that was distributed and the responses that were obtained from the cohorts are included in the appendix.

4.2 Sampling Method

There are two approaches to sampling, namely probability and nonprobability (Walker, 2014). According to Jackson (2011) probability sampling means each member of the population has an equal probability of being selected to be part of the sample. Three of

the most commonly used random sampling methods are simple random sampling, stratified random sampling, and simple random cluster sampling (Fink, 2009).

The most suitable sample for this research appeared to be the stratified sample as it works well with subgroups. It requires the calculation of the proportion of each of the studied subgroups (in this research, doctors, managers and IT professionals) and determines whether the samples (the respondents from the three subgroups) are representative, given that the total number of each subgroup is known. Fink (2009) defined the stratified random sampling method simply as: “Subdivide the population into subgroups or strata and select a given number or proportion of respondents from each stratum to get a sample”. (p. 53)

4.2.1 Sample Size

In this research, three categories or subgroups were chosen as they were most likely well- experienced in their field and in the use of EHRs. As shown in Table 2, below, KFSH employs 93 managers, 635 doctors, and 132 IT professionals; a total of 860 employees with these job titles (KFSH, 2015).

SurveySystem online calculator (Creative Research Systems, 2012) was used to calculate the sample size of the total number of the population with confidence level of 95% and confidence interval of 5%. The online calculator indicated that the sample size should be 266 participants.

The formulas used in the sample size calculator are:

$$s = \frac{Z^2 * (p) * (1 - p)}{C^2}$$

$$new\ ss = ss / (1 + (ss - 1) / pop)$$

Where:

Z = Z value (e.g. 1.96 for 95% confidence level)

p = percentage picking a choice, expressed as decimal (.5 used for sample size needed)

c = confidence interval, expressed as decimal (e.g., .05 = ± 5)

pop = population

4.2.1.1 Steps of Stratifying the Sample Size

The following steps were used to identify the required sample size for each subgroup (Statistics How To, 2015).

Step 1: Stratifying the population. Staff were divided into strata in accordance with their profession: doctors, managers, and IT professionals.

Step 2: Strata are represented in a table.

Table 2 Number of each stratum

Staff	Total Number of Staff in Strata
Managers	93
Doctors	635
IT professionals	132
	Total = 860

Step 3: Define the sample size. This step was completed, as shown above, and the calculated sample size was 266.

Step 4: Use the stratified sample formula. (Sample size of the strata = entire size of sample / population size * layer size). As indicated in table 3 below.

Table 3 Calculation of the required sample size

Staff	Number of staff in Strata	Number of staff in Sample
Managers	93	$266/860 * 93 = 29$
Doctors	635	$266/860 * 635 = 196$
IT Professionals	132	$266/860 * 132 = 41$
Total = 266		

Step 5: Random sampling. Simple random sampling was executed (i.e. the survey questionnaire was distributed randomly in each stratum).

For this study, the total number of the needed sample was 266 KFSH staff.

4.3 Data Analysis

Lime-Survey automatically sorted and calculated the percentages of the data as they were being updated. The totals and percentages were calculated manually and salient percentages were observed and highlighted accordingly. Graphs and tables were generated via Microsoft Office Excel 2010.

The type of data analysis utilised in this research is known as descriptive statistics or descriptive data analysis (Fink, 2009) as it involves describing the data or statistics in hand using graphs and percentages to identify any patterns of the results. This type of data analysis is beneficial for comparing and contrasting the results.

4.4 Ethical Considerations

Prior to conducting this study, a Massey University Human Ethics Application form was completed and submitted to the Massey University Human Ethics Committee (MUHEC). The survey was commenced after gaining the committee's approval as it was deemed low risk (Appendix B).

No names, emails, or any identifying information of the participants was included in the research. To assure their confidentiality, the data were accessible via a login name and a password that only the researcher knows. The data will be disposed of one year after the completion of the research.

4.5 Summary

This research uses a quantitative methodology and the online Lime-survey tool to explore the views of staff at KFH on EHR related topics including confidentiality, privacy, and policy and cultural and religious issues, as well as their recommended access method to EHR. Three professions at KFSH were chosen to complete the survey, doctors, managers and IT professionals, and the reasoning behind choosing those three professions and for choosing KFH were discussed in this chapter.

Also in this chapter, the sampling size of the three professions was calculated. This research was approved by the MUHEC as it was deemed of low risk and privacy and confidentiality of the participants was assured as an integral part of the survey.

Chapter 5

Results

To gain a better understanding about the current EHR access control utilised in KFSH and to explore how acceptable BPI or non-biometrics technologies are among staff (doctors, managers and IT professionals), a quantitative, cross-sectional, online survey methodology was utilised, as explained in Chapter 4.

This chapter consists of three main parts: validity of results, presentation of the results of the survey; and a summary of the chapter. The presentation of the results is divided into six parts, in accordance with the six sections of the survey, and is illustrated via pie and bar charts with a summary for each section.

5.1 Validity of Results

Table 4 Number respondents and sample size

Staff	Actual number of staff in KFSH	Calculated sample size	Number of respondents
Managers	93	29	16
Doctors	635	196	111
IT Professionals	132	41	23
Total	860	266	150

There were 150 Managers, doctors and IT professionals who responded to this survey; this is about 17.5% of the actual total number of those sectors at KFSH. Most of the respondents were doctors (111) and the least were managers (16) as shown in Table 4, above. Table 4 shows the calculated sample size (as calculated in Chapter 4) and the figures in that column represent the least number of participants needed in order for the results to be representative. The above table clearly shows that the number of

respondents in each staff sector is less than the desired, calculated sample size. Therefore, the results of the survey cannot be representative.

5.2 Survey Results

The first part of the survey results presents the background, or demographic, information of the research participants, including how long they have been working in health care for. The second part is dedicated to presenting information about current access patterns at the hospital. The third part of this chapter shows the results on the existing access control mechanisms used in the hospital. The fourth part illustrates the results regarding the participants' views and recommendations in relation to biometric access control. The fifth part presents information in relation to the participants' level of awareness of EHR policies and privacy and security breaches. Finally, the sixth part presents the impact of religion and culture on EHRs as perceived by the participants.

5.2.1 Participants' Backgrounds at KFSH (Section A)

This section of the questionnaire was designed to gather background information about the survey respondents. It consisted of four questions, referred to as A1, A2, A3 and A4.

Q. A1: What is your profession in the hospital?

This question was designed to stratify the staff members working at the KFSH. As illustrated in Figure 8, 74% of the respondents were doctors, while 11% of the staff were engaged in hospital management, and 15% were employed in the IT department.

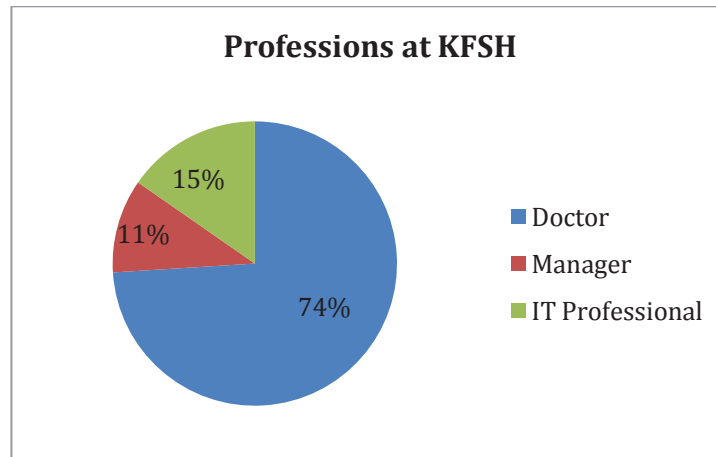


Figure 8 Different professionals at KFSH (Q A1)

Q. A2: Are you a Saudi citizen?

The second question was whether the participants were Saudi citizens. 65% indicated that they were non-Saudi citizens in contrast to 35% who indicated that they were Saudi citizens.

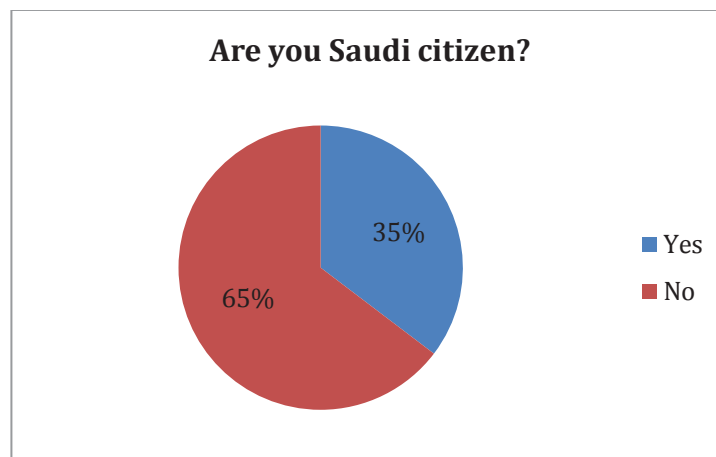


Figure 9 Number of Saudi and non-Saudi participants (Q A2).

Q A3: How long have you been working in health care?

The third question stratified the staff according to their duration of service at the healthcare. Of those that responded, 4% indicated that they had been working in health care for less than six months, while 15% indicated that their health care work experience was more than six months but less than one year. Most of the respondents (81%) indicated that their healthcare experience was more than two years. In essence, it

can be assumed that most of the respondents have a fair level of experience with EHR usage and any relevant policy. Figure 10 illustrates the distribution of the staff according to their duration of service.

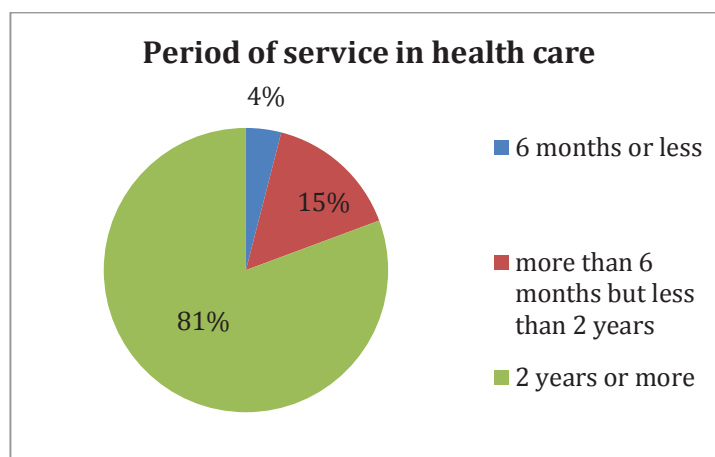


Figure 10 Length of service/ work experience of participating staff in health care (Q A3).

Q A4: How long have you been using Electronic Health Records (EHRs)?

Question 4 in section A highlighted the experience of the respondents in using EHRs. 64% indicated that they had two years or more experience with using EHRs in comparison to 32% who indicated that they had between six months and two years' worth of experience. Only 4% had six months or less experience.

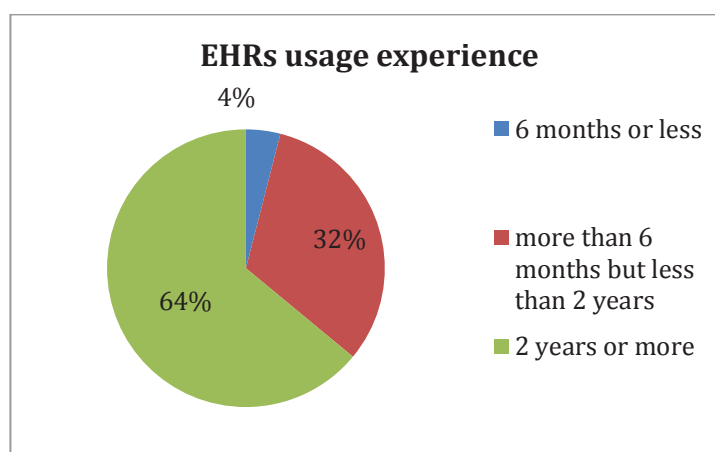


Figure 11 Experiencing using EHRs of KFSH staff (Q A4).

5.2.1.1 Summary of Section A

In general, almost three quarters of the respondents are doctors and most of the respondents have two or more years experience in the healthcare field. Approximately two thirds of the participants were non-Saudi and the rest were Saudi.

5.2.2 EHR Current Access Patterns at KFSH (Section B)

This section was dedicated to understanding the EHR usage patterns at the KFSH. The survey questions were designed to highlight if EHR use was implemented at the hospital and the different sections of the staff that had access to the patient records. This section also gathered the opinions of the respondents about data security and integrity at the KFSH. This section consisted of four questions, referred to as B1, B2, B3, and B4.

Q B1: Does your hospital store patient records electronically?

The first question under section B gathered the opinion of the respondents on whether KFSH stores and manages EHRs. All of the respondents indicated that patient records were stored electronically. This may indicate that all the respondents are aware of the processes concerning data access and the security policies that are in place for data integrity and security.

Q B2: How much access do you have to Electronic Health Records (EHRs)?

Question B2 tried to determine the level of awareness of the hospital's access policy by asking the respondents about how much access they think they are entitled to (no access, limited access, or full access). Responses were gathered from doctors, managers, and IT professionals individually, along with the overall response count. As shown in Figure 12, below, all of the doctors and IT professionals indicated that they believed they had full access to the electronic patient records, in comparison to only 25% of the managers.

The majority of managers (75%) thought they had limited access to the records. None of the respondents indicated that they had no access.

Overall, 91% of the staff thought they had full access, while 9% believed they had limited access to the records, as illustrated in Figure 13 below.

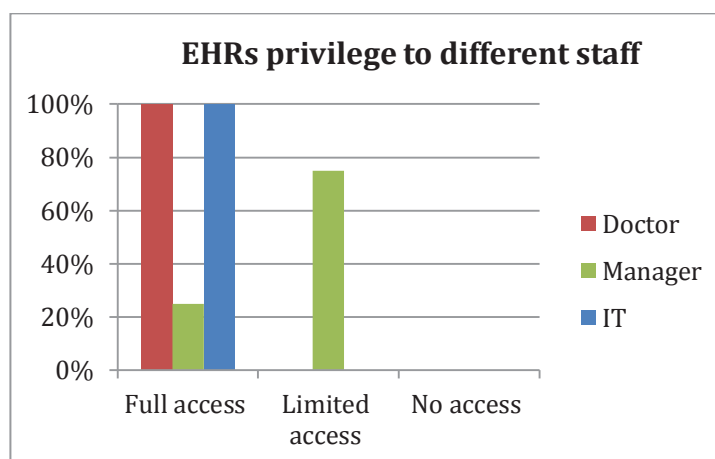


Figure 12 Level of access of different staff to EHRs (QB2).

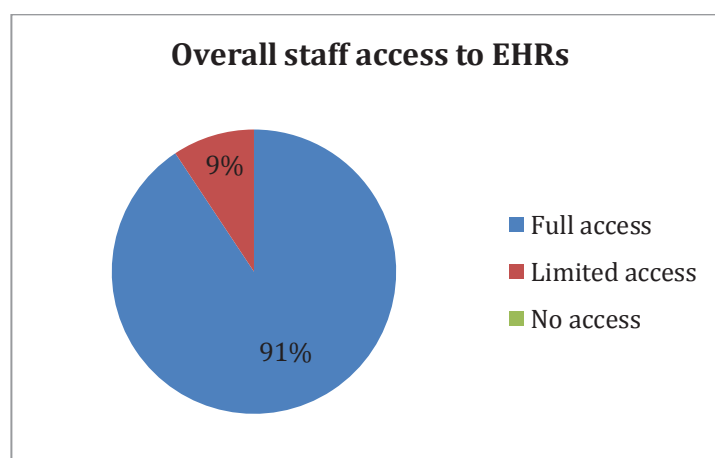


Figure 13 Overall access to EHRs (QB2).

Q B3: In your opinion, what is the main reason for accessing EHRs?

Approximately 85% indicated that the main reason for accessing EHRs was for work purposes in comparison to 15% of the respondents who indicated that the main reason for accessing EHRs was for a favour to a friend or family member. None of the

participants indicated that they accessed EHRs for personal interests. The responses are illustrated in Figure 14, below.

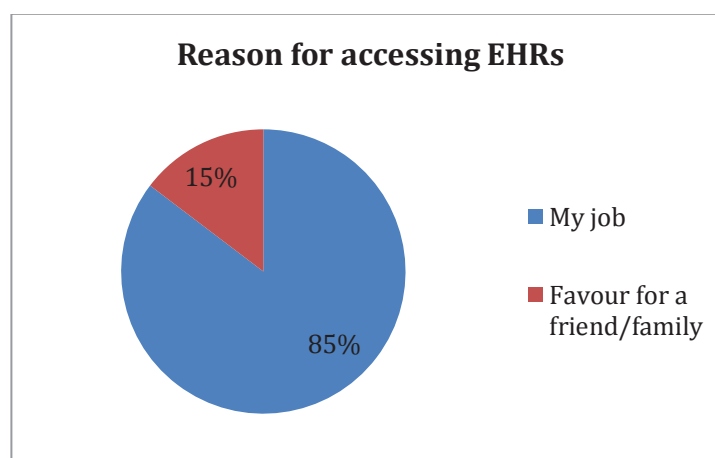


Figure 14 Reason for accessing EHRs by different staff members (Q B3).

5.2.2.1 Summary of Section B

All of the respondents indicated that the hospital stores patient records electronically and all of them had some level of access to EHR. Doctors and IT professionals believed they had full access, as opposed to managers whose opinions varied about their access between full and limited. Approximately 15% of the participants indicated that they would access EHRs as favour for friends and family; this is a concern as staff need to be fully aware about the importance of privacy and confidentiality of patient records, including EHR.

5.2.3 Existing access control mechanism at KFSH (Section C)

Section C of the questionnaire was dedicated to exploring the methods used to access electronic patient records at the KFSH. This section focused on the different biometric and non-biometric techniques that were used in the hospital to access data electronically. This section consisted of three questions, referred to as C1, C2, and C3.

Q C1: Usually, what type of method is used to access EHRs in the hospital?
(Participants may choose more than one answer)

Question C1 tried to determine the EHR access technique implemented at the KFSH. As shown in Figure 15, all of the respondents replied that non-biometric techniques were used to access the records. These results highlight that biometric access techniques may not be yet implemented in the hospital.

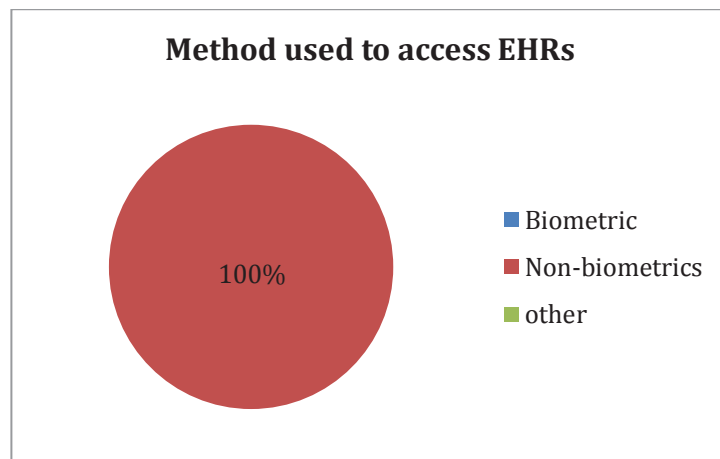


Figure 15 Method used to access EHRs at KFSH (QC1).

Q C2: What biometric tool(s) are used in the hospital? (Participants may choose more than one answer)

The answer to this question was expected in context to the responses obtained from question C1. As shown in Figure 16, all of the respondents indicated that biometrics are not used in the hospital at all as all of the participants selected 'not applicable'.

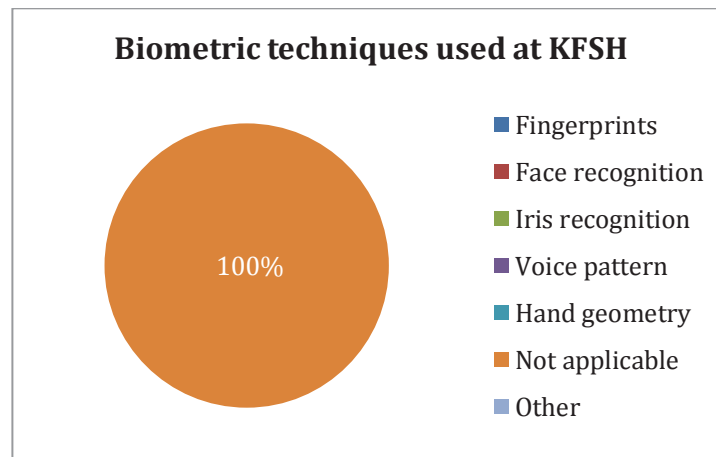


Figure 16 Biometric techniques at KFSH (Q C2).

Q C3: What non-biometric tool(s) are used in the hospital? (Participants may choose more than one answer)

Question C3 highlighted the non-biometric techniques that are used at the KFSH for accessing patient records. The answers of the respondents, illustrated in Figure 17 below, indicated that password-protected access was the type of non-biometric method currently used in the KFSH.

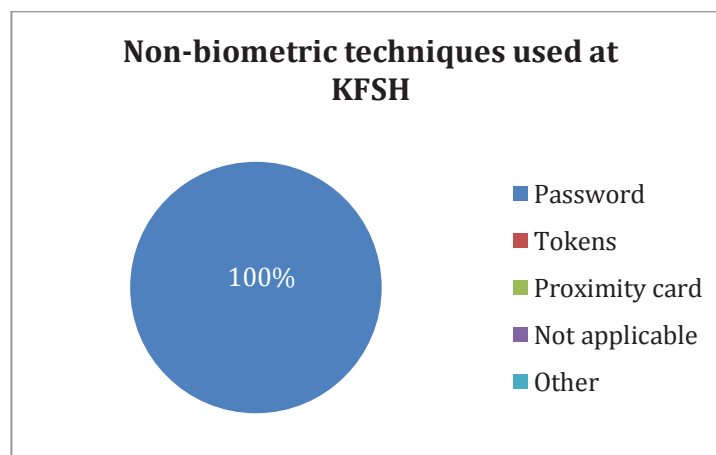


Figure 17 Non-biometric techniques used at KFSH (Q C3).

5.2.3.1 Summary of Section C

The data in this section showed that the access mechanism used in the hospital to access EHR is non-biometric; namely; password as opposed to biometric access technologies.

5.2.4 Views/ Recommendations on Biometric Access Control (Section D).

The objective of this section was to determine the viewpoints of the respondents on the suitability of different biometric techniques for EHR access. Question D1 (SQ 1, 2, 3) asked the respondents if they believed that BPI systems were more efficient and secure for accessing EHRs. Question D1 (SQ 4, 5) attempted to determine if culture and religion had an impact on selecting the BPI system for EHR access. Finally, questions D2 and D3 highlighted the recommended and most appropriate BPI technique for Saudi male and female patients. This section consisted of three questions, referred to as D1 (SQ 1-5), D2 and D3.

Q D1 (SQ1): To what extent do you agree with the following statements: [Biometric patient identification systems provide more security to EHRs].

Figure 18, below, highlights the answers of the respondents to question D1 (SQ1). From the figure it can be clearly inferred that the majority of the respondents either agree or strongly agree with the fact that the BPI system provides more security for EHR access than non-biometric systems.

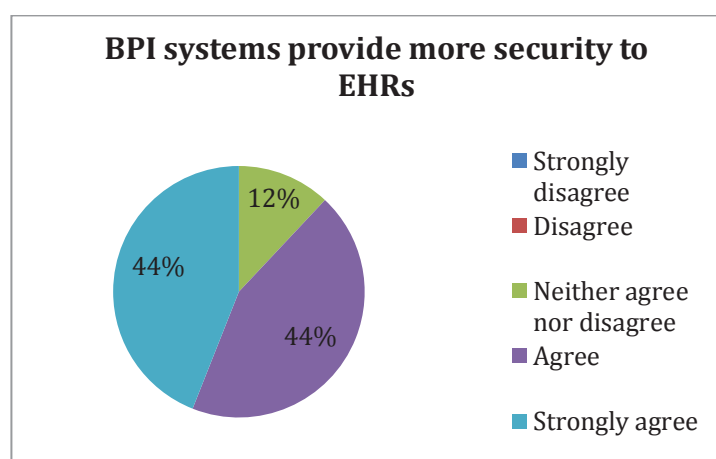


Figure 18 Opinion on whether BPI systems are more efficient in providing access security (Q D1: SQ1).

Q D1 (SQ2): To what extent do you agree with the following statements: In hospitals, biometric patient identification systems would be more preferable than non-biometric systems].

This question asked the respondents if they thought BPI systems would be more preferable in hospitals to non-biometric access methods. Once again, an overwhelming 90% of the respondents agreed that BPI systems are more preferable in comparison to other access methods or systems. The responses are illustrated in Figure 19, below.

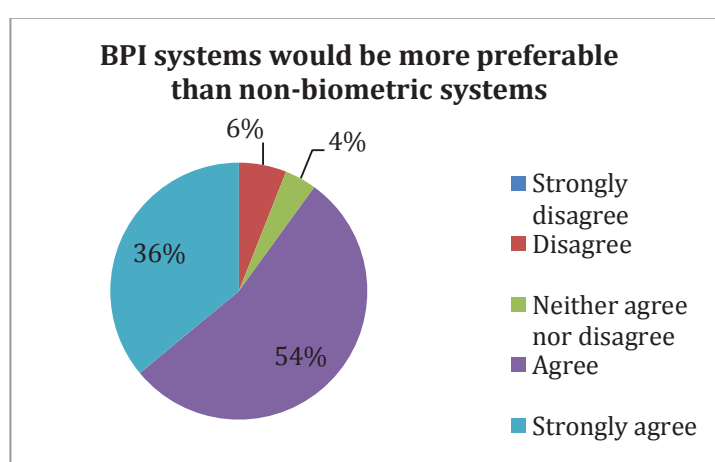


Figure 19 Opinion on preferable techniques (Q D1: SQ2).

Q D1 (SQ3): To what extent do you agree with the following statements: [Biometric patient identification systems are more efficient than paper-based systems].

Question D1 (SQ3) asked the respondents if they believe that BPI systems are more efficient in providing secured data access compared to paper-based systems. The answers were expected in context of the answers to D1 (SQ1 and SQ2) and, as shown in Figure 20 below, 96% of the respondents replied that they agree or strongly agree.

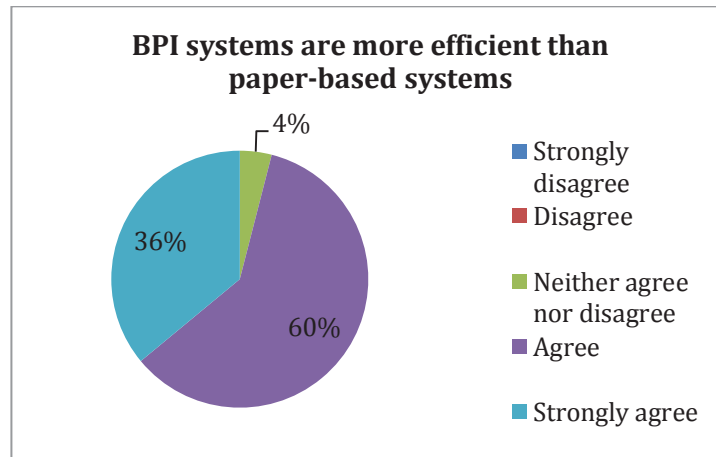


Figure 20 Opinion between BPI systems and paper-based techniques (Q D1: SQ3).

D1 (SQ4): To what extent do you agree with the following statements: [Culture would have an impact on the use of biometric technologies that utilise body feature(s) of patients in hospital]

Question D1 (SQ4) attempted to highlight the impact of Saudi culture on the use of BPI systems as they involve the scanning of body features of patients at the KFSH. Figure 21 below shows that 33% of the respondents believed that culture would have an impact (either agreed or strongly agreed), 27% disagreed, while 40% answered ‘Neither agree nor disagree’. Figure 22 shows that almost all the Saudi participants either agreed or strongly agreed that culture would have an impact on the use of biometric technologies that use body feature or features of patients in hospitals. In contrast, all of the 40% who answered ‘Neither agree nor disagree’ were non-Saudi and a large proportion of them (24%) disagreed.

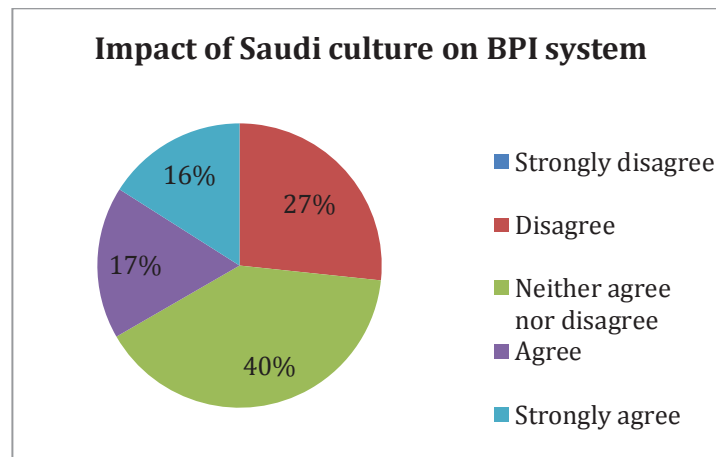


Figure 21 Opinion on whether Saudi culture has an impact on BPI (Q D1: SQ4).

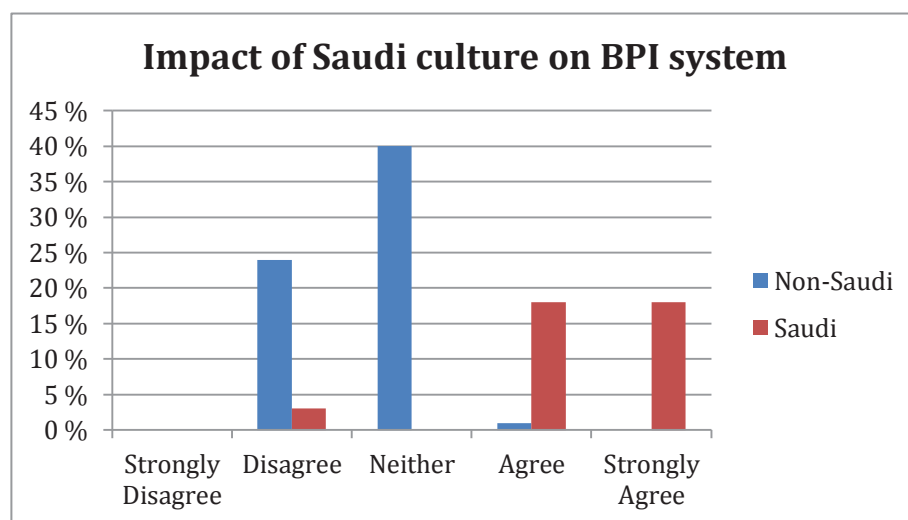


Figure 22 Opinions of Saudi and non-Saudi participants on whether Saudi culture has an impact on BPI (Q D1: SQ4).

D1 (SQ5): To what extent do you agree with the following statement: [Religion would have an impact on the use of biometric technologies that utilise body feature(s) of patients in the hospital].

This question highlighted the significance of religion on the use of BPI system in KFSH. The responses indicated that opinions were evenly distributed between disagree and neutral; with 44% believing that religion had no impact and 44% remaining neutral. In contrast, 12% believed that religion would have an impact. Figure 23 below, illustrates the opinions of the respondents to this question.

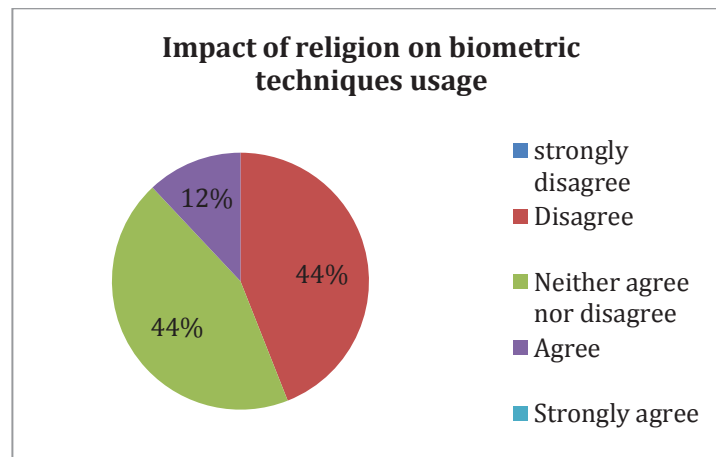


Figure 23 Opinion on whether religion would have an impact on BPI system usage (Q D1: SQ5).

D2: In your opinion, what type of biometric system(s) would be suitable for Saudi male patients in the hospital? (You may choose more than one answer).

Question D2 tried to determine the biometric technique that respondents believed was best suited for Saudi male patients. The results, illustrated in Figure 24, indicated that fingerprint scanning and hand-palm veins scanning were the most recommended biometric techniques, followed by face and iris recognition and voice recognition. None of the participants selected 'I do not know'.

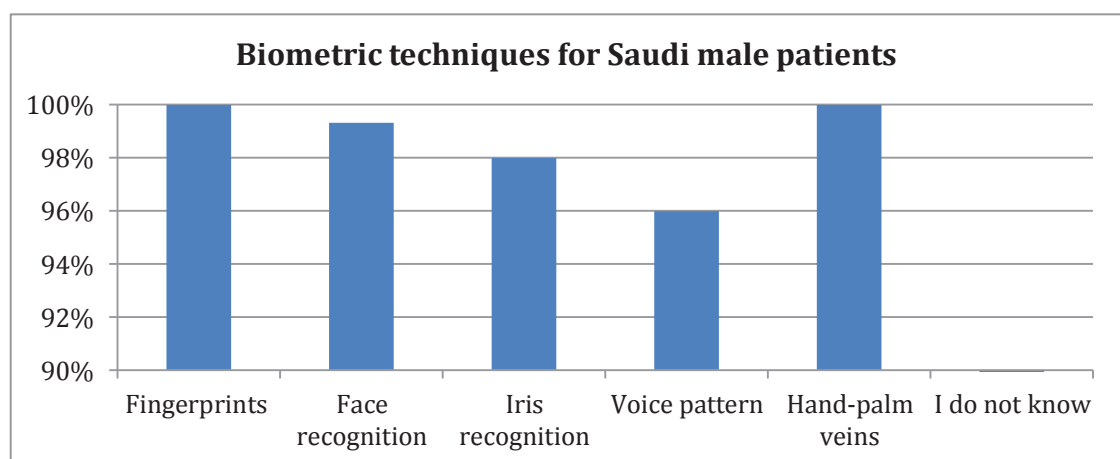


Figure 24 Biometric techniques suitable for Saudi men (Q D2).

D3: In your opinion, what type of biometric system(s) would be suitable for Saudi female patients in the hospital? (You may choose more than one answer).

In terms of the biometric techniques that were best suited for Saudi female patients, the results, illustrated in Figure 25, show that the respondents recommended fingerprint scanning technique the most, followed by hand-palm veins and voice recognition. Face recognition was not recognised as a viable option for Saudi female patients (2%). Once again none of them chose 'I do not know'.

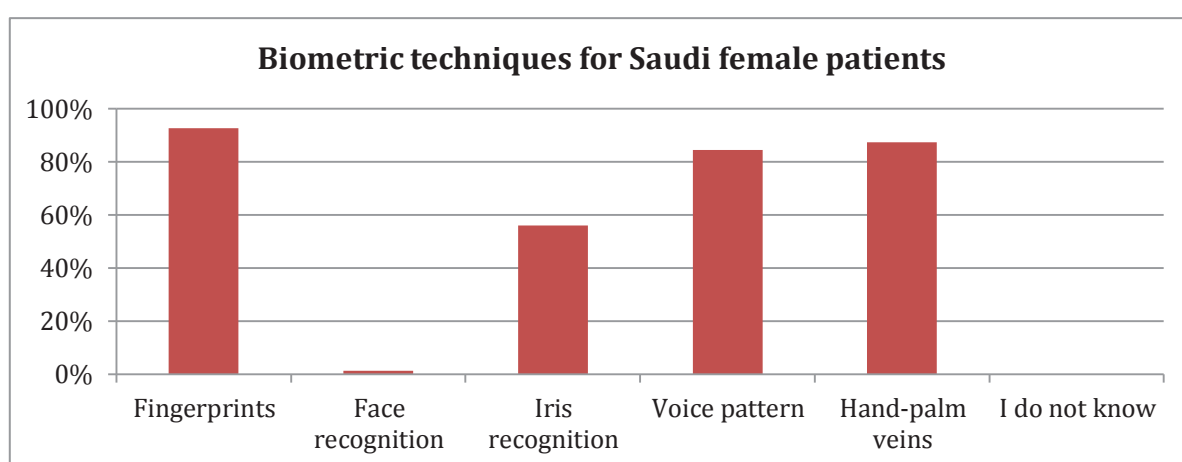


Figure 25 Biometric techniques suitable for Saudi women (Q D3).

5.2.4.1 Summary of Section D

Answers to questions in this section indicated that the participants recommended a BPI system which involved the use of body features of patients over non-biometric systems to access EHRs, and that they perceived BPI systems to be more secure and more efficient than paper-based methods. The results clearly show that staff at the KFSH had a very positive view on BPI systems and identified the advantages of the paradigm. Participants' views on the impact of religion and culture on BPI technologies were quite diverse, with approximately 40-44% of the participants neither agreeing nor disagreeing to any impact by the two. Opinions of Saudi participants and those of the non-Saudi participants on the impact of culture on BPI technologies were much polarised as the

Saudi participants believed that there is an impact while the non-Saudi participants either disagreed or neither agreed nor disagreed.

Furthermore, all the participants indicated that fingerprints, or voice pattern biometric techniques or methods would be most appropriate for Saudi male patients. Most of the participants also thought that other BPI methods (face recognition, iris recognition, and hand-palm veins) would also be appropriate. In contrast, face recognition was considered the least appropriate access method for Saudi female patients, followed by iris recognition.

5.2.5 Staff views on risks of EHR Security and Privacy Breaches and policies in the KFSH (Section E).

The objective of this section was to determine the viewpoints of the respondents on the security of EHRs in the KFSH. The respondents were asked if they were aware of the security policies that were in place at the hospital and if, according to them, the access policies and protocols were robust enough to fully secure patient data. Given the high stakes in ensuring data confidentiality, the questions in section E tried to determine if the implemented security policies were fully understandable to the respondents and if there were possibilities that confidential data might be revealed to friends and family. This section essentially tried to determine if the staff were confident of the security measures that were currently in place in KFSH. This section consisted of questions E1, E2, E3 and E4 (SQ 1-3).

Q E1: Have you been given any EHR security policy document?

Question E1 asked the respondents if they were ever given any security policy document defining the steps that need to be followed to ensure patient data security and integrity. The majority of the respondents (98%) indicated that they had received such a

document and that they were aware of all the protocols that needed to be followed. A minority (2%) replied that they were not in possession of any EHR security policy document. Figure 26, below, illustrates the responses of the respondents to question E1.

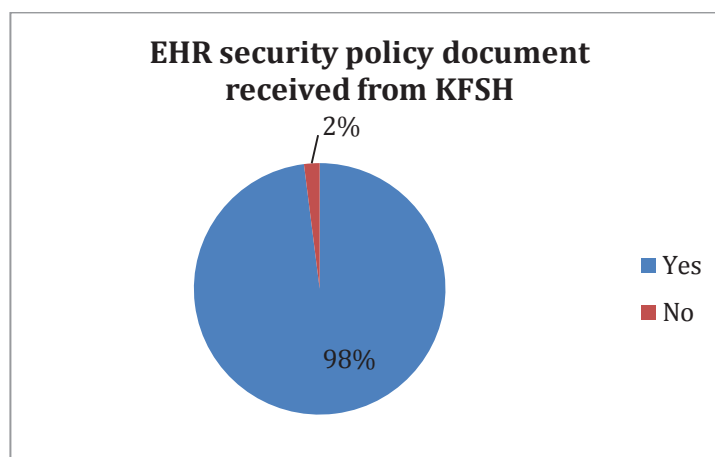


Figure 26 Responses of the KFSH staff on whether they received any EHR security policy document (E1).

E2: Do you believe that the EHR security policy protects the privacy of EHRs efficiently?

As a follow up to question E1, the respondents were asked if they thought that the security policy that was in place protects EHRs efficiently. Around, 85% of the respondents, as illustrated in Figure 27 below, said that this is the case, in comparison to 15% who said the opposite.

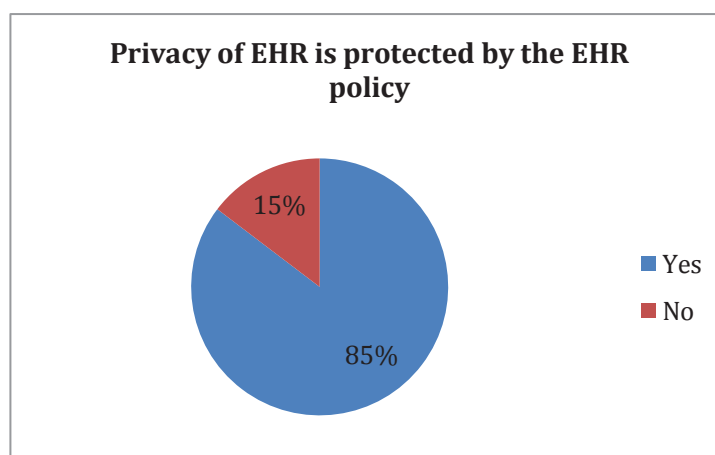


Figure 27 Opinion of the respondents on whether the policy protects the privacy of EHRs (E2).

E3: Do you believe that the EHR security policy protects the confidentiality of EHRs efficiently?

Question E3 attempted to gather the opinions of the respondents on whether the hospital security policy was efficient at protecting EHR confidentiality at KFSH. An overwhelming 86% of the respondents said the policy protects confidentiality efficiently and 14% said this was not the case. Figure 28 illustrates the responses of the respondents to question E3.

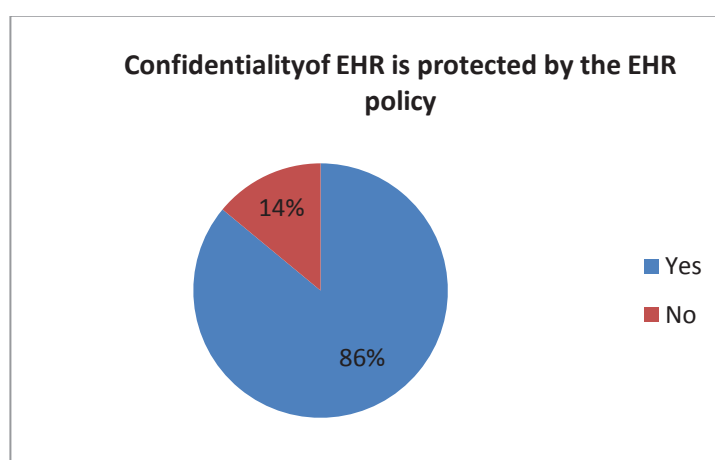


Figure 28 Opinion of the respondents on whether the policy is efficient in protecting EHR confidentiality (E3).

E4 (SQ1): To what extent do you agree with the following statements: [The EHR security policy procedures are fully understandable among staff].

Given the fact that majority of the respondents are confident in the hospital system security policy, question E4 (SQ1) asked if all the security policy procedures were properly understandable to them. The majority of respondents (90%) said that they fully understood the procedures (illustrated in Figure 29 below). This observation is in agreement with the responses to the previous question, where 86% of the respondents indicated that they were confident in the system security policy of the KFSH regarding protection of EHR confidentiality.

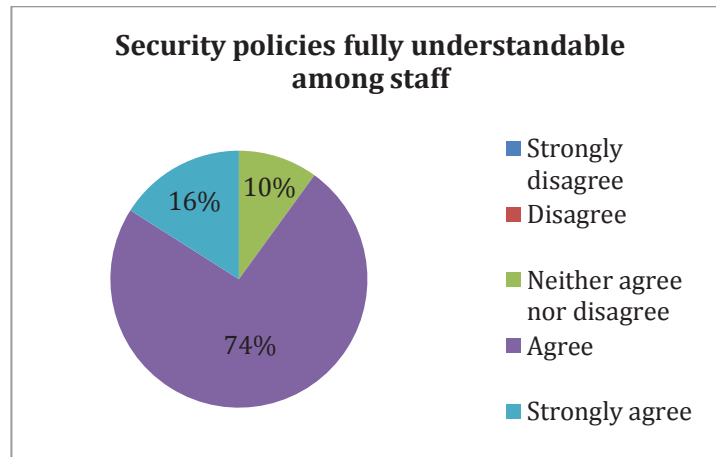


Figure 29 Opinion of the respondents on whether the security procedures are fully understandable to them (QE4: SQ1).

E4 (SQ2): To what extent do you agree with the following statements: [EHRs can be revealed to any of the patient's family without the patient's consent].

This is a critical question that tried to determine if there was any breach in data confidentiality by the staff at the KFSH. The respondents were asked if it was possible to reveal EHRs to any of a patient's family without consent. While 30% agreed that records could be revealed, 60% did not give a definitive answer. A small group of respondents (10%) disagreed that EHR data could be revealed to patient's family members without consent. Figure 30, below, illustrates the fragmented opinion of the respondents to this question.

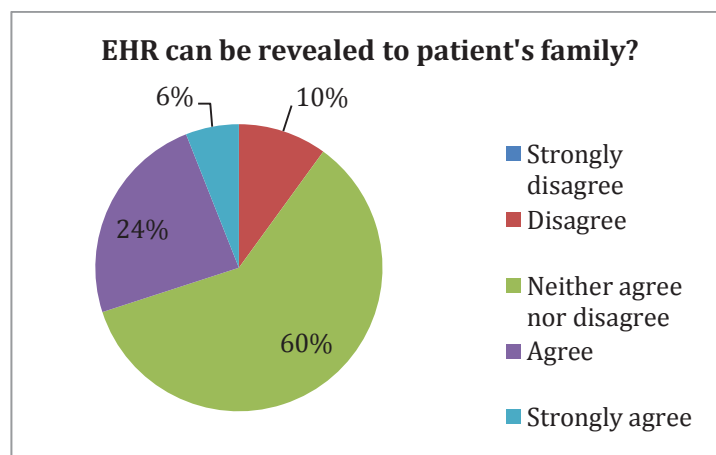


Figure 30 Opinion of the respondents on whether EHR data can be revealed to patient's family (QE4: SQ2).

E4 (SQ3): To what extent do you agree with the following statements: [EHRs can be revealed to any of the patient's friends without the patient's consent].

Just like the earlier question, question E4 (SQ3) is also very critical in the context of protecting privacy and integrity of patient data. The respondents were asked if electronic patient records could be revealed to any of the patient's friends without consent. Half the respondents either disagreed or strongly disagreed that patient data could be revealed to patient's friends, while 40% remained neutral. A small group (10%) said that patient data could be revealed to friends. Figure 31 illustrates the responses to question E4 (SQ3).

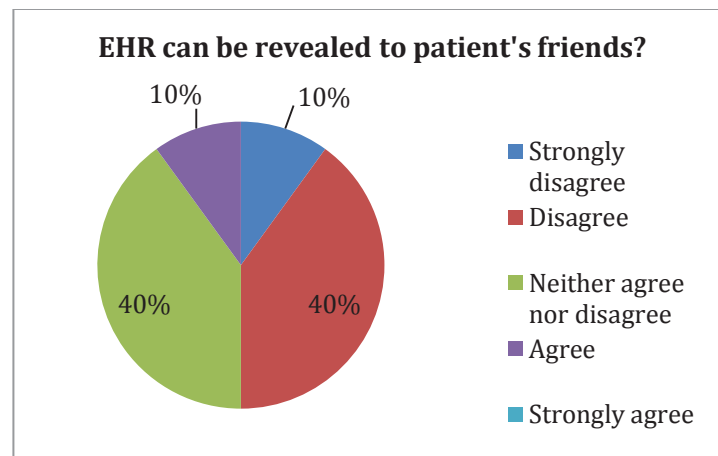


Figure 31 Opinion of the respondents on whether EHR data can be revealed to patient's friends (QE4: SQ3).

5.2.5.1 Summary of Section E

2% of the participants indicated that they did not receive any EHR policy document. Three quarters of the participants believed that the EHR security policy protects confidentiality and privacy of EHRs efficiently and only 10% of the participants indicated that the security policies are not understandable. 30% of the participants agreed or strongly agreed to the statement that EHR could be potentially revealed to patients' family and 10% agreed that they can be revealed to friends. The majority of the responses to the last two questions indicated that the participant neither agreed nor

disagreed. This again indicates there may have been some doubt about the clarity of the question posed, as the circumstances of the revelation were not specified.

5.2.6 Perception of Staff on the Impact of Religion and Culture on privacy and confidentiality of EHRs (Section F).

This final section of the survey questionnaire focussed on the impact of religion and Saudi culture on the privacy and confidentiality of patient data. The section also included questions that asked the hospital staff if they showed diligence in protecting the privacy and integrity of patient data. Finally, the focus was also given to the aspect of threats to life through any breaches in the privacy of EHR data. This section consisted of question F1 (SQ 1-6).

Q F1 (SQ1): To what extent do you agree with the following statements: [Cultural issues have a great impact on EHR privacy and confidentiality].

The first question of section F asked the respondents if Saudi culture had any impact on EHR privacy and confidentiality in the KFSH. Almost half of respondents (48%) believed that culture does have an impact, while 42% believed that there is no impact by culture on EHR privacy. Figure 32, below, illustrates the responses to question F1 (SQ1)

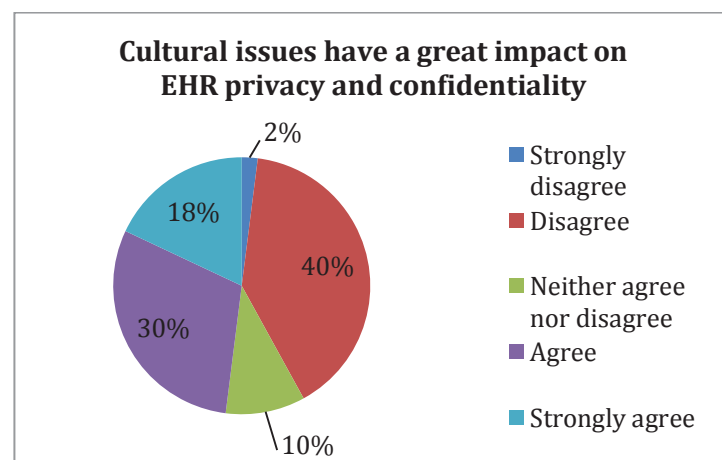


Figure 32 Opinion of the respondents on whether cultural issues have an impact on EHR privacy and confidentiality (QF1: SQ1).

Q F1 (SQ2): To what extent do you agree with the following statements: [Religious issues have a great impact on EHR privacy and confidentiality].

Question F1 (SQ2) asked the respondents if religion had any impact on EHR privacy in the KFSH. Over half of the respondents (60%) believed that religion does not have an impact (either disagreed or strongly disagreed), while 36% believed that it did have an impact on EHR privacy. Figure 33, below, illustrates the responses to question F2 (SQ2).

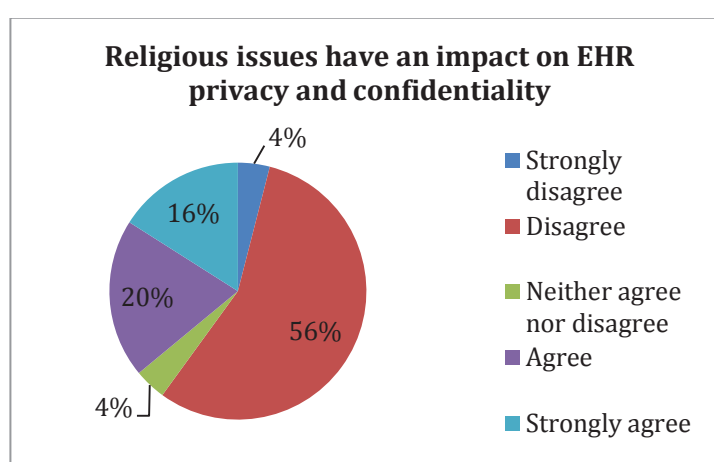


Figure 33 Opinion of the respondents on whether religion has an impact on EHR privacy and confidentiality (QF1: SQ2).

Q F1 (SQ3): To what extent do you agree with the following statements: [Health staff are fully committed and responsible for protecting patients' privacy and confidentiality].

Does the staff at the KFSH act responsibly and diligently to protect patient's EHR privacy and confidentiality? Encouragingly, 92% of the respondents indicated that they showed good resolve in ensuring that patient's EHR privacy and confidentiality were properly protected. A small number of respondents (4%) however indicated that this was not the case. Figure 34 illustrates the responses to question F1 (SQ3).

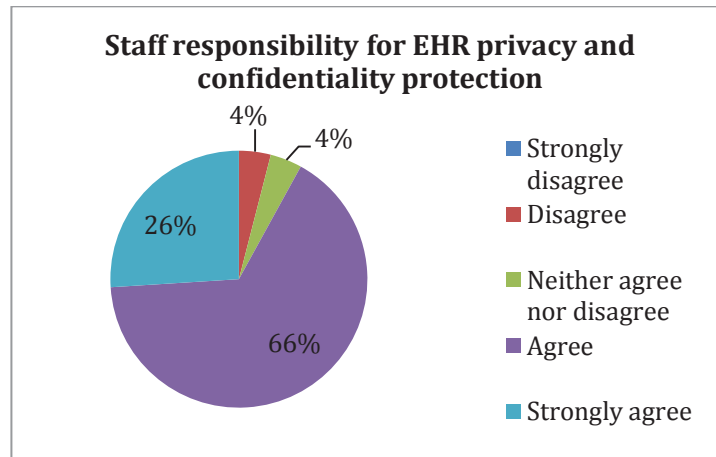


Figure 34 Opinion of the respondents on whether health staff show responsibility for protecting patients' EHR privacy and confidentiality (QF1: SQ3).

Q F1 (SQ4): To what extent do you agree with the following statements: [Saudi patients take cultural issues related to their privacy and confidentiality seriously].

Question F1 (SQ4) gathered the opinion of the respondents on whether cultural issues related to privacy and confidentiality are very important to Saudi patients. While 24% remained neutral, 66% of the respondents indicated that Saudi patients take cultural issues relating to their privacy and confidentiality seriously. The results are illustrated in Figure 35, below.

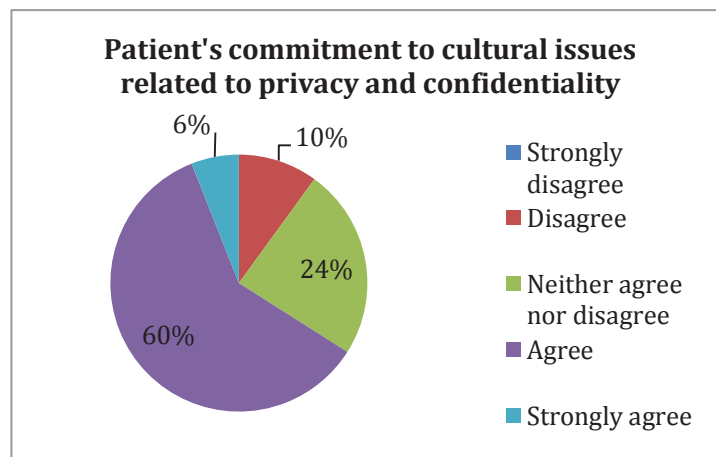


Figure 35 Opinion of the respondents on whether Saudi patients are fully committed to cultural issues related to privacy and confidentiality (QF1: SQ4).

Q F1 (SQ5): To what extent do you agree with the following statements: [Saudi patients take religious issues related to their privacy and confidentiality very seriously].

Question F1 (SQ5) focused on the significance of religion to Saudi patients regarding privacy and confidentiality of EHR data. As illustrated in Figure 36, below, 42% agreed that religious issues related to privacy and confidentiality were very important to Saudi patients, while 50% of the respondents did not have any opinion. Only 8% of the respondents indicated that religious issues were not important.

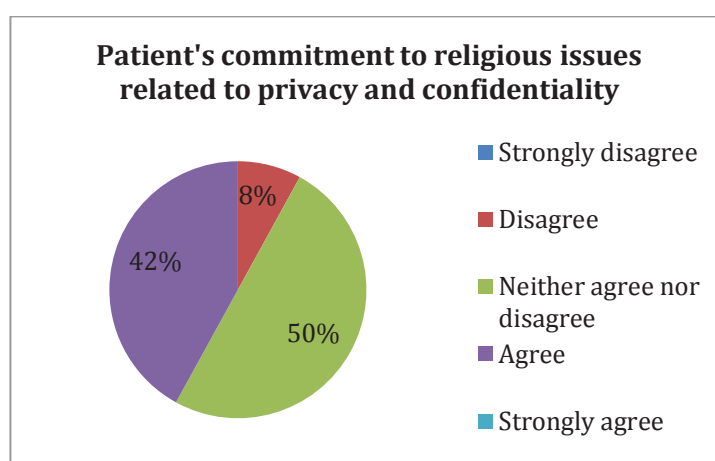


Figure 36 Opinion of the respondents on whether Saudi patients are fully committed to religious issues related to privacy and confidentiality (QF1: SQ5).

Q F1 (SQ6): To what extent do you agree with the following statements: [Revealing a patient's EHR to a family member without patient consent may expose patient's life to danger].

The last question in the survey under section F asked the respondents if any breach of electronic patient records could jeopardise the life of patients in Saudi Arabia. Of those who responded, 38% agreed with the observation that revealing Saudi EHRs might expose patient's life to danger, while 60% gave no opinion. A small 2% replied that they perceived no threats to patients' lives if patients' records were revealed without the patient's consent. All the respondents who agreed or strongly agreed to the above

statement were Saudi; on the other hand, most of the respondents who disagreed or selected neither were non-Saudi. The results are illustrated in Figure 37 and Figure 38 below.

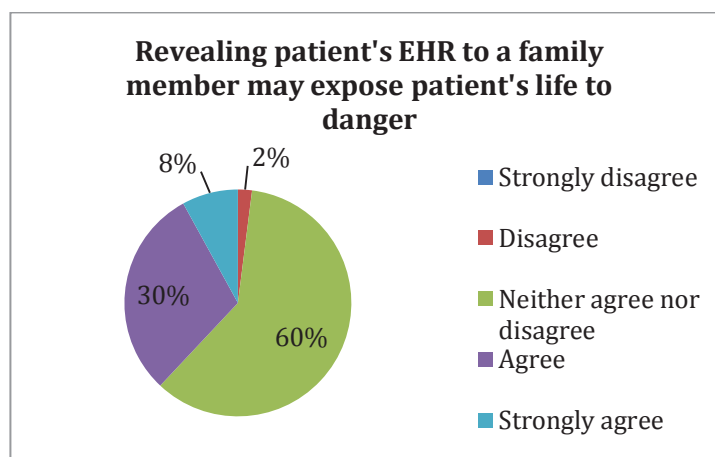


Figure 37 Opinion of the respondents on whether revealing Saudi EHRs might expose patients' life to danger (QF1: SQ6).

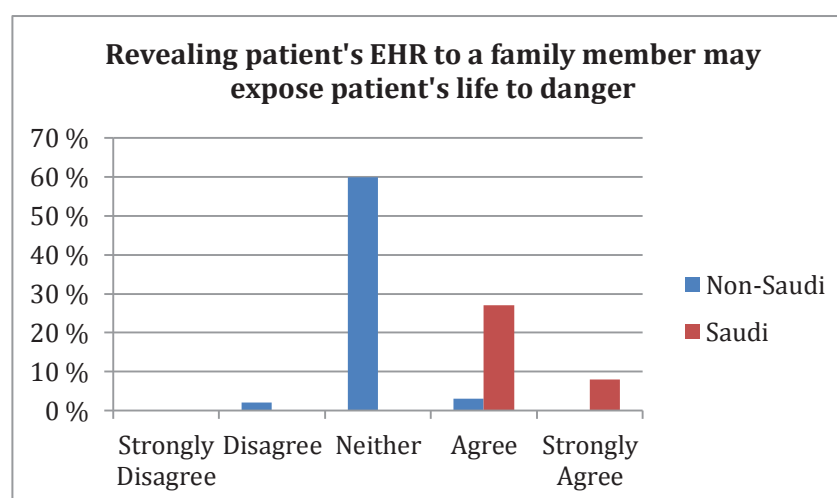


Figure 38 Saudis and non-Saudis opinions (QF1: SQ6).

5.2.6.1 Summary of Section F

To summarise section F, a small portion of the respondents indicated that the health staff were not fully committed to the protection of patient privacy and confidentiality. Similarly, a small percentage of those who disagreed that revealing patient EHRs to a family member without the patient's consent might expose the life of the patient to danger, were non-Saudi participants. Once again opinions of Saudi participants and

those of their non-Saudi counterparts were polarised with Saudi participants who believed that revealing patients' EHR to family would endanger the lives of patients and the non-Saudi participants who, in large, did not have an opinion on the matter or disagreed with it. Almost half of the participants thought cultural issues had a great impact on EHR privacy and confidentiality and more than one third thought that religion also had an impact.

5.3 Summary of Chapter

In general, the results show staff at KFSH view biometric technology favourably, perhaps due to its superiority in securing EHRs, as the current access technology that has been utilised is simple password protection. The results also indicate that staff trust the current EHR security policy that is currently in place at the KFSH.

All of the explored BPI technologies in this research were perceived as acceptable for Saudi male patients to use, however opinions on these technologies for women varied, with the face recognition technique being the least favoured. These findings were unexpected as this research hypothesised that non-biometric techniques would be more favourable, as they are less physically intrusive.

The results indicate some level of confusion about confidentiality and privacy of patients and EHRs in the context of the strict cultural and religious Saudi context, even though most of the respondents had two or more years of experience in healthcare settings. This could be associated with staff negligence or perhaps lack of cultural and EHR policy awareness and needs to be further explored by the hospital to effectively remedy these issues, including adequate training.

Chapter 6

Findings and Discussion

The purpose of this chapter is to discuss the findings of this research, presented in Chapter 5. The present research was undertaken to ascertain how acceptable BPI technology would be if introduced in Saudi Arabia, taking into consideration culture and religion, as well as confidentiality and privacy of EHRs. This was done by surveying staff at the KFSH to understand their perspectives on these issues, as there is a lack of research around this topic in a Saudi hospital context.

This chapter consists of six sections: the first section details the background of the cohort and the demographic data of the survey; the second section highlights staff perceptions in relation to EHR security; the third section discusses staff awareness of data access technologies and relevant policies; the fourth section focuses on the views of the respondents regarding different features of the BPI technology and their level of confidence on that new technology - this is discussed in light of the second research hypothesis; the fifth section discusses the the unauthorised revelation of EHRs to family members, as well as other relevant findings; the sixth, and final, section is dedicated to exploring the impact of culture and religion on EHRs, as featured in the findings.

6.1 The Background of the Cohort

The survey questionnaire that was distributed among the staff of the KFSH included thirty questions divided into six sections. Altogether 150 individuals responded to the survey, out of which 111 were doctors, 16 were managers, and 23 were IT professionals.

Section A questions were designed to stratify the respondents according to their work profile. As already mentioned, the majority of the respondents were doctors (74%),

followed by IT professionals (15%), and managers (10%). Given the fact that these doctors reported they had full access to the EHRs (as did the IT professionals), their survey responses should provide great insight into discovering the challenges facing the implementation of BPI systems in relation to Saudi culture.

The staff members who participated in the survey would only be able to provide comprehensive and viable responses if they had sufficient work experience in healthcare, as it is expected to reflect a good level of EHR usage. Encouragingly, greater than 80% of the respondents had more than two years' experience in healthcare and 32% had a service period between six months and two years. Also, 64% of the respondents indicated that they have been using EHR at the hospital for more than two years. Most of the participants were non-Saudi and only 35% of them were Saudi.

From these results it can be assumed that staff with more than two years of experience will have a reasonable idea on the best method of EHR access that will ensure appropriate privacy and confidentiality and may satisfy the social cultural norms of Saudi Arabia, in addition to full understanding and appreciation of the system and its strengths and shortcomings.

6.2 The Perception of EHR Security Among the Respondents in KFSH

As stated by Ozair et al., (2015), one of the most prominent concerns or arguments against the adoption of technologies, such as EHRs, is their perceived lack of adequate security measures to ensure data privacy and integrity.

The questionnaire provided a snapshot of EHR usage/access patterns and policies at the KFSH. Since EHRs are very sensitive information, it is important that staff are fully

aware of proper access restrictions and that appropriate protocols are in place stipulating who can and cannot access them.

All the doctors and IT professionals survey respondents stated they had full access to EHRs. Based on these responses it is assumed that all the doctors and IT professionals at KFSH, or at least a significant portion of them, have full/unrestricted access control. In comparison, managers responded that they only had partial access to the EHRs.

Hustinx (2010, cited in Rezaeibagha, 2013) argued that patients would have increased trust in health professionals and the health care system if they knew that their EHRs were well protected. Ninety percent of those surveyed in this research affirmed that they believed that the EHRs were safe at the KFSH. This indicates that these respondents were fully confident about the security measures that were in place. However it would have been better if 100% of the staff were fully confident with the security measures. The results indicated that 5% of the respondents were not sure if the records are safe and another 5% indicated that the EHRs were not safe in the hospital. This is something that should be investigated further to understand the reasons behind this, especially given that the MOH in Saudi Arabia has ambitious plans to extensively develop EHRs in the country (Almalki et al., 2011); therefore there should not be any complacency surrounding the security of EHRs in Saudi Arabian health centres or institutions.

Given the sensitive nature of patient data, access to EHRs should be strictly limited and there should be a valid reason for the files to be accessed. De Bord et al. (2013) argued that the relationship between staff and their patients could be damaged when patients realised their privacy and confidentiality had been breached. This, in turn, could make patients hesitant to fully confide in their health professional and, as an outcome, this would impact on the accuracy of the records (De Bord et al., 2013). Question B3 tried to

determine the participant's reasons for accessing EHRs. More than 85% of the respondents indicated that the main reason behind data access was for work purposes, however, rather worryingly, around 15% of the respondents indicated that they had accessed the records as a favour to family and friends. This breaches the privacy and confidentiality of patients and it calls for proper staff training.

6.3 Staff Awareness on Data Access Technologies and Policies

Section C of the survey focused on the technical aspect of data access protocols implemented in the hospital with regards to EHRs. As outlined in the literature review, biometric methods have not yet been used in Saudi hospitals, despite the huge potential for it; biometric technologies have been implemented in other major governmental and private sectors in Saudi Arabia. In line with this all of the respondents indicated that the method used to access EHRs was a non-biometric password.

It is important to understand the reasons why biometric techniques have not been adopted at the KFSH despite the fact that the Saudi government has been promoting the acceptance and adoption of biometric technologies in both government and private sectors (Alhussain & Drew, 2009) and is also working on the creation of the largest biometric hub in the world (Arab News, 2014). The reasons could be wide and varied, such as lack of technical expertise, cultural and religious obligations or constraints and apprehensions about adopting a new technology and further studies are needed to ascertain the reasons. Given the fact that biometric recognition systems utilise physical or anatomical features of an individual for recognition (Perrin, 2002), some identification technologies, such as face scanning could be an issue in Saudi Arabia as was deemed fine for men but not for women as the responses indicated. However, in the context of the advantages of BPI techniques over non-biometric techniques and the

availability of options that can oblige with all the religious and cultural concerns, it is about time that changes are brought in with regards to how EHRs are accessed and managed. Most importantly, the BPI techniques are far more capable of ensuring the integrity of patient data, as it makes certain critical health information is recorded in the correct EHR, an aspect that is of paramount importance from the cultural and religious point of view in Saudi Arabia.

6.4 Security Concerns and Staff Confidence on the New Technology

Before a new technology is implemented in an organisation it is extremely important to understand the viewpoint of the people who would use that technology, as they may have reservations regarding the new technology or protocols that guide it. Additionally, since the Saudi government is committed to the expansion of biometric technology (for example, the creation of the largest biometric hub in the world) (Arab News, 2014), it is important to capture the level of awareness of staff about such technology and to capture their general opinions regarding the change that is being anticipated.

The background study and literature review carried out during this study have highlighted the advantages of BPI techniques over non-biometric ones and using this knowledge as a background, section D of the survey questionnaire tried to obtain the opinions of the respondents on different aspects of BPI techniques that may be implemented in the hospital. As already mentioned, one of the aims of this study was to explore the feasibility of implementing BPI techniques for access of EHRs in Saudi healthcare centres. So, apart from the technical concerns, other elements such as religion, tribal culture, and massive urbanisation are critically important to understand the situation in Saudi Arabia (Abdullah et al., 2006).

The security of EHRs is a fundamental concern for any hospital and encouragingly, 88% of the respondents in this research indicated that they believe that BPI systems provide more security to patients' EHRs than non-biometric systems. This indicates that the staff of KFSH are open to the new technology and recognise the benefits that biometrics can bring to their organisation with regards to data security. It also highlights a positive attitude towards new technology and supports the observations made in the literature review that Saudi Arabia is witnessing a tremendous growth in the biometrics market, as explained by Aldajani (2012).

In the survey, 90% of the respondents clearly believed that BPI systems were recommended to non-biometric systems. Furthermore, an overwhelming 96% said that BPI systems were preferable to traditional paper-based systems. It can be seen that the respondents in the survey were aware of the advantages, which supports the Arab News (2014) study, but the concern remains as to why biometric techniques have still not been implemented. This finding disproves one of the study hypotheses, which suggested that biometrics would be less favourable due to its intrusiveness.

6.5 The Impact of Saudi Culture and Religion on Biometrics

The forth question in section D tried to shed some light on this aspect and asked the respondents if they believed that Saudi culture has an impact on the use of biometrics technology. While 27% said that culture was not an issue, 33% indicated that culture does present some hurdles, and 40% had no opinion on what was asked. The results indicated disparity in opinion about the matter between Saudi participants who almost all of them believed there is cultural impact and non-Saudi participants whom mostly disagreed or neither agreed nor disagreed.

While the Saudi culture is known to be relatively conservative and that biometric techniques involve scanning of anatomical body parts, it would be assumed that the culture might actually have an impact on the use of biometrics. When the same question was asked for religion, 44% of the respondents said that it had no impact while 12% said that religion is a concern. In contrast, 44% had no opinion on the question; which could be understandable since the implementation of BPI technology has not been realised in Saudi hospitals, or at least in KFSH, and thus many professionals cannot assert, based on experience, if culture and/or religion would have an impact on the perspective technology.

It is important to understand if the choice of BPI techniques can, or will, have an impact given the religious and cultural context, for example the significance of the hijab for Saudi women. When respondents were asked about the most suitable BPI technique for Saudi male patients, all the different BPI techniques received almost equal preference, but when the same question was asked for Saudi female patients, 92% of the respondents opted for fingerprints. Around 85% said that voice pattern recognition was a good option for females, while 87% indicated that hand-palm veins scanning was also very good. When it came to iris recognition, only 56% found this suitable for females, even though it does not involve removing the hijab. This could be explained by Saudi culture, where a sect of Islam requires a different type of female head cover, including a kind of hijab that covers the entire face as well as the eyes. Therefore, it can be assumed that iris technology would not be appropriate for such women, as it requires uncovering the eyes.

As far as face recognition is concerned, almost all participants said that it was not suitable for Saudi female patients. The reason behind such overwhelming response may,

yet again, relate to lifting the hijab, which is not acceptable from a religious and/or cultural perspective. So, in essence, the deep-rooted cultural and religious constraints appear to have an impact and if the right BPI techniques are not implemented then they will not find any acceptance at the KFSH, or any other healthcare institutions in Saudi Arabia. However, this study cannot establish in concrete terms if the lack of acceptance of face recognition for women was due to cultural or religious influences and the matter needs to be investigated further through other studies.

As stated in the literature review, Saudi Arabia is a very prominent Islamic nation and strictly implements a strict dress code for women in compliance with a rigid version of Sharia law. It is an absolute necessity that women wear an abaya, a, and headscarf at all time in public places. This means that all the facial features of a woman are covered and techniques such as face recognition will not work, as it requires scanning of the entire face (Al-Harby et al., 2009). This is definitely a barrier but it does not mean that the Saudi healthcare centres cannot implement the new technology and perhaps the technology could be modified in a way that would maintain cultural and religious norms in Saudi hospitals.

Gostin et al. (2009) emphasised that institutes would benefit from better protection of privacy of patients and state-of-the-art web security when they install a biometric system. In general, if the appropriate technique is installed that is acceptable to both Saudi men and women, the BPI techniques could get extensive acceptance, leading to increased safety and security of EHRs at Saudi healthcare institutions.

At this stage it is very well established that security is of paramount importance when it comes to managing EHRs. However, to make sure that the privacy and integrity of the

data is intact at all times, hospital staff should fully appreciate the need to uphold security policies that are in place to protect the patients and their data.

6.6 EHR Policy

Almost all the respondents surveyed had been provided with the security policies currently in effect at the hospital and more than 85% of the respondents agreed that the policies were effective in ensuring the privacy and integrity of EHRs. However, almost quarter of the participants indicated that the EHR security policy does not protect EHRs efficiently and neither agreed or disagreed with the statement: ‘security procedures are fully understandable among staff’. These answers may indicate that EHR security policy could be confusing to some staff and may need to be amended. The fact that almost quarter of the participants agreed to the statement that ‘EHRs can be revealed to any of the patient’s family without patient’s consent’ and 10% agreed to ‘EHRs can be revealed to any of the patient’s friends without patient’s consent’ also emphasises confusion with regard to EHR security or privacy.

In comparison, a study by Aldajani (2012) in King Faisal Hospital, another major Saudi hospital, highlighted the lack of an EHR security policy in that hospital. This highlights two possibilities: the first, is that not all Saudi hospitals lack EHR policies; the second, is that there have been some major developments in EHR security policy in hospitals in Saudi Arabia since Aldajani’s study was completed; thus it reflects positively on privacy and confidentiality of patients and their records.

Even though there is a clear understanding that biometric systems are very effective, the majority of the respondents indicated that they trusted that the current EHR security policy was capable of protecting the privacy and confidentiality of EHRs. As it may take some time before BPI techniques are fully implemented in the hospital, patients

and the staff can continue to take advantage of EHRs for efficient care management and delivery, saving lives and resources. This study does not reflect the actual effectiveness of the privacy policies of the hospital, but rather shows the confidence of the staff in those policies.

Critically, about one third of the respondents agreed (agree or strongly agree) that EHRs could be revealed to patient's families, while 10% agreed they could be revealed to patient's friends without consent. It is difficult to draw conclusions and assumptions from these data without knowing what the hospital's consent policy is, which better fit the Saudi cultural and/or religious norms as opposed to Western norms. A future study that analyses information on the EHR security policy at KFSH would be advantageous in revealing how much such a policy is influenced by Saudi norms versus Western norms.

6.7 Unauthorised Revelation of EHRs

In Saudi Arabia, unauthorised revelation of sensitive medical information, including EHRs, could expose patients' lives to danger, or even death, as discussed in the literature review in Chapter 3. Therefore, it is vital that hospital staff, especially doctors and managers, have a robust understanding of the Saudi culture, and its norms in the context of the hospital's policy around privacy and confidentiality. The results, however, were surprising: 60% did not have an opinion on such a sensitive issue (neither agreed nor disagreed), 2% disagreed and only 38% agreed (agreed or disagreed). This is a serious matter that needs to be addressed by the hospital through proper training in Saudi culture for non-Saudi staff. Such a need becomes obvious when considering that all of the participants who disagreed or showed no opinion on the matter were non-Saudi and the lack of opinion in this situation could reflect confusion or unsureness.

Perhaps because those respondents realised that there are times during which patients are unable to give consent, for example if they are in a coma or are suffering dysarthria. Due to this ambiguity, the majority of the respondents may have found it very difficult to answer this question.

6.8 The Impact of Culture and Religion on EHR Privacy and Confidentiality

Saudi Arabia is a deeply religious nation with the holiest Muslim cities in the world: Mecca and Medina. Religion is the way of life there and it virtually affects every aspect of people's daily routine. The Saudi culture, the time-tested and rigid social norms, and the age-old traditions of Saudi society are crafted by Islamic values and the question of a new technology finding acceptance depends entirely on whether it fulfils the religious obligations (Al-Saggaf, 2004).

So, in essence, although culture and religion appear to be taken very seriously in Saudi society this study revealed an almost even divide in views, with 48% of respondents agreeing (strongly agree or agree) that cultural issues have a great impact on EHR privacy and confidentiality, in comparison to 42% of respondents who either disagreed or strongly disagreed. Interestingly a similar but smaller divide in opinion was revealed in relation to religious issues, as 60% of the respondents said that religious issues had no impact on EHR privacy and confidentiality in comparison to 36% who said that religion does have an impact.

Participants were also asked about their opinions on whether patients take cultural and religious issues, in relation to their privacy and confidentiality, seriously. To this, 66% of the participants agreed or strongly agreed that cultural issues were taken seriously by the patients, in contrast to only 10% who disagreed. On the other hand, 42% of

participants agreed that patients take religion seriously, in contrast to only 8% who disagreed and 50% who neither agreed nor disagreed.

Earlier in the survey it was seen that when it came to selecting the best BPI technique for Saudi women, the choices were very limited. The significance of the hijab became evident and this indicates the importance of culture and religion in the Saudi culture. The real responsibility for protecting the privacy and integrity of EHRs lie with the staff who have access to the data and handle them on a regular basis. If they do not fully appreciate the privacy concerns, the data can never be safe; the responses that were received from the survey respondents 90% indicated they felt responsibility for protecting patients' EHR privacy and confidentiality. This is a very positive finding and it is promising to think how safe the data will be with more robust biometric data access techniques. However the 4% of respondents who disagreed is rather alarming, as even one breach in privacy and confidentiality of EHR could be a matter of life and death. This requires proper training for staff on the seriousness of privacy and confidentiality, as well as their role in protecting them.

The religion of Islam stresses the importance of privacy confidentiality or the 'protection of secrets' and forbids backbiting (Alahmad & Dierickx, 2012), which in a sense forbids harm to individuals through revelation of their secrets or private information. Perhaps this can be extended to include confidentiality and privacy of patients and their medical records. However, a clear medical Fatwa that protects the rights, privacy, and confidentiality of patients is needed by prominent Islamic institutes, such as The International Islamic Fiqh and the Islamic Fiqh Council in the Muslim World League. Such a Fatwa could resolve the sense of confusion about privacy and confidentiality and could guide related policies.

6.9 Recommendations

This study could form the basis for numerous future studies on BPI technology in hospitals and on the matters of EHR confidentiality, privacy, and policy as follows:

1. Interviewing staff about privacy and confidentiality and EHR to obtain in-depth knowledge about their attitudes, cultural, and religious awareness, as well as their own values (cultural and religious background) and how they impact on privacy and confidentiality of patients and EHRs.
2. A study that analyses information on EHR policy at KFSH compared to international policies on these matters. The study could also analyse any Islamic or cultural influence that contributed to the making of the policy and investigate the views of staff on different aspects of it.
3. A pilot study that introduces one or more biometric/BPI technology at KFSH or any other major Saudi hospital and obtains feedback from the patients and staff, the preference of the staff, and the preference of patients (if more than one technology was used).
4. Full KFSH staff training on culture awareness; especially for non-Saudi staff.
5. Full KFSH staff training on privacy and confidentiality and safety aspects in relation to when the privacy and/or confidentiality can be broken.
6. A study that captures the views of other relevant sectors of staff at KFSH such as nurses. A mixed quantitative and qualitative methodology could provide quick, affordable, and more comprehensive data about the participants' views on issues of policy confidentiality and privacy in Saudi hospitals.

Chapter 7

Conclusion, implications and limitations

This study has been successful in establishing the effectiveness of BPI techniques in protecting patient data and it also indicates that staff at the KFSH also fully acknowledge the same. One of the two hypotheses of this study stated that most of the Saudi staff would prefer the less intrusive, non-biometric techniques over BPI techniques but the results of the survey indicated the opposite; most of the participants preferred BPI techniques and had a high level of confidence about the technology in terms of security and efficiency, although apparently biometric technology has not yet been used in the hospital. The results suggest that the staff appreciated or were aware of the advantages of BPI technology. Perhaps a good way of determining how successful BPI technology would be in the KFSH is through a pilot study that introduces different interfaces of the technology in the hospital and asks participating patients and staff about their experience with using the technology, whether they liked it or not, and whether they found it culturally or religiously appropriate. A mixed methodology with room for comments and open-ended questions about the technology would be very informative and would be highly recommended for future studies in that field.

This study has been also successful in determining the participants' recommendations for different types of BPI technologies, such as hand-palm veins, voice pattern, and fingerprints, taking into account gender differences. For example, the least preferred BPI technique among female participants was the face recognition, which probably reflects the cultural expectations and religious obligations in Saudi society. Although more data would be needed in order to generalise the results, the results are quite

informative for any future implementation of BPI techniques in the KFSH or any other medical institutes in Saudi Arabia.

One major implication of the findings was that the implementation of new BPI techniques should take into consideration the cultural and religious obligations prevalent in Saudi Arabia in order to succeed. For example, if the appropriate biometric access technique was chosen for women that, for example, do not involve lifting of the hijab, it is highly likely that it will find great acceptance in healthcare centres and medical institutes. Given the fact that BPI techniques are more recommended, in terms of security and efficiency, compared to the non-biometric techniques, it could be argued that it is not a matter of choice but an absolute necessity to implement the same at the KFSH at the earliest.

Once again, the results indicated that culture and religion have a major role to play and the main factors impacting implementation of a BPI system concerning privacy and confidentiality of Saudi EHR became clearly evident. Data breach is a very sensitive issue in Saudi Arabia, however only 38% of the participants in this study agreed such a breach could endanger lives of patients, in comparison to 2% who disagreed, and 60% who neither agreed nor disagreed. This result is surprising because the previous answers of the participants suggested that they had a good level of understanding of the Saudi culture and religion but the answer to this question suggested some ignorance about aspects of the Saudi society. It was also surprising because 80% of the participants had two or more years of work experience at the KFSH. It should be iterated that even though only 2% disagreed to this, such a result is very significant because mismanagement of EHRs could result in death. For instance, if a doctor was dealing with a female patient who was pregnant before she married, without the knowledge or

consent of her parents, and her EHR showed that her next of kin is her father who does not know about her pregnancy, informing the father about the pregnancy of his daughter could result in the honorary killing of the daughter, as per the real life example given by Galanti (2004).

An important implication of the findings of this study is the need for proper and comprehensive training for staff on how to deal with privacy and confidentiality of patients, as well as trainings on cultural norms and religious expectations. Understandably so, this is based on the presumption that not all the doctors and other staff are Saudis.

So, for successful implementation, the cultural and religious issues that need to be taken care of are thoroughly addressed and demarcated. In light of these observations, it can be stated that the study was able to answer all the research questions that were defined at the beginning of the study. There is no doubt that there are cultural and religious issues surrounding the most appropriate BPI technique for the female gender but once that is addressed, it is anticipated that biometric protocols will receive excellent acceptance at the hospital.

While there are established non-biometric techniques to access EHRs at the KFSH, state-of-the-art BPI systems could significantly improve the safety and integrity of EHRs

With regards to limitations, it can be stated that the results would have been more statistically significant if a larger cohort had taken part in the survey, as only 150 participants responded to the survey while the calculations of the sample sizes in Chapter 4 showed that 266 participants were needed for the data to be representative.

Thus, the number of the participants was smaller than the sought sample size. Though this makes it hard to generalise due to the lack of results validity, the findings of this research were quite interesting and cannot be ignored.

Another important limitation of this research is that the views of nurses, a big sector of professionals in hospitals, were not sought and captured. Possibly the results would have been different or more diverse if that was the case. This is an aspect that has not been given the required focus in the survey.

The quantitative methodology chosen for this research was not the best and a mixed (quantitative-qualitative) questionnaire would have been much more informative. This a major limitation of this research that should have been thought about during the planning stages of the research. A more powerful methodology is structured interviews with staff and patients, however, this was beyond the budget of the researcher and may have created ethical issues.

Responses to some of the questions highlighted some major issues in the question design as, for instance. 60% of the respondents neither agreed nor disagreed with the statement that EHRs can be revealed to family. Clearly, there are occasions during which staff are left with no option but to reveal an EHR to family, and even seek consent from them, as the patient could be in a state of coma; the 60% may reflect ambiguity or confusion about the question. This major limitation could have been identified and avoided if the survey was piloted before the questionnaires were distributed. Also, it would be more powerful if the research had explored under what circumstances EHRs could be accessed or revealed.

On an overall basis, the study presented a comprehensive view of the issues pertaining to successful implementation of BPI techniques at KFSH and the possible solutions that can ensure a speedy acceptance. There is no doubt that more avenues can be explored to obtain an even more exhaustive view of the situation but the observations that were made during the study will definitely serve as a good knowledge base for future courses of action.

This research had two primary aims: the first was to discover the views and attitudes of staff with regard to EHR confidentiality, privacy, and policy and whether this was influenced by religious and cultural issues. It is concerning that some answers to the survey questions indicated negligence, ignorance, or confusion about what confidentiality and privacy mean. For example, 15% of the participants indicated that they would access EHRs as favours for their friends or family, which breaches the privacy of patients. The extent of the problem could be much larger as the number of participants (doctors, managers, and IT professionals) was only 150 out of 860 employees. The data showed that perhaps there is less confusion about policy, as most of the participants agreed that the EHR security policies and procedures were fully understandable by staff. This could in effect reduce the likelihood of confusion and instead highlight negligence. One should note here that BPI technology itself would not resolve the problem of accessing EHRs as favour for friends or family, however in the future the BPI technology could be expanded to include staff biometrics which has the potential to improve the confidentiality of patient records. The study has been successful in determining issues in relation to EHR privacy and confidentiality but perhaps it could not fully capture the views of the participants on the issues and an alternative methodology, such as interviews, or mixed methodology with open-ended questions about EHR privacy, confidentiality, and policy in the Saudi context would

have been more appropriate. The results above indicate a possible lack of commitment of staff with regard to confidentiality and privacy in the Saudi Arabian context; this commitment could not be asserted.

The second aim was to explore which of the two systems, BPI or non-biometric, would be more recommended by staff. This study has been very successful in determining the participants' recommendations and strikingly, all of them recommended the BPI technology over the non-biometric technology that is currently in use. The participants were allowed to select more than one option and face recognition was the least favourite BPI option for Saudi female patients, in contrast to Saudi male patients where there was very little difference in preference. This finding was also unexpected as the second research hypothesis predicted that the majority of the participants would recommend non-biometric technologies as they are less intrusive than its biometric counterparts.

In terms of research questions, the study has been successful in determining the participants' recommended access method, as discussed earlier, but was not as successful in capturing their views on confidentiality and privacy. The study has also succeeded in determining the existence of the impact of Islam and Saudi culture on privacy and confidentiality but the level and nature of this impact remains unknown.

In summary, this study was designed to provide a glimpse into the views of health care professionals (doctors, managers, and IT professionals) at the KFSH on selected aspects of EHR. The first aspect was the existing non-biometric EHR technique currently utilised in the hospital and the level of their awareness of relevant security policies in place. The second aspect explored whether or not staff recommended BPI techniques and which techniques were recommended. The study hypothesised that BPI techniques would be less recommended than non-biometric due to the intrusive nature of the

former. The third aspect examined whether or not religion and culture impact on EHR policy, privacy, and confidentiality.

References

- Abdullah, A., Rogerson, S., Fairweather, N. B., & Prior, M. (2006). The motivations for change towards e-government adoption: Case studies from Saudi Arabia. Paper presented at the eGovernment Workshop.
- Alahmad, G., & Dierickx, K. (2012). What do Islamic institutional fatwas say about medical and research confidentiality and breach of confidentiality? *Developing world bioethics*, 12(2), 104-112.
- Aldajani, M. (2012). Electronic Patient Record Security Policy in Saudi Arabia National Health Services. (Doctoral Thesis). Available from: <https://www.dora.dmu.ac.uk/bitstream/handle/2086/6016/thesis%20aldajani%202012.pdf?sequence=1>
- Al-Harby, F., Qahwaji, R., & Kamala, M. (2009). The effects of gender differences in the acceptance of biometrics authentication systems within online transaction. Paper presented at the CyberWorlds, 2009. CW'09. International Conference.
- Al-Hijaili, S. A. J., & AbdulAziz, M. (2011). Biometrics in health care security system, iris-face fusion system. *International Journal of Academic Research*, 3(1), 11-19.
- Alhussain, T., & Drew, S. (2009). *Software Services for e-Business and e-Society*. C. Godart, N. Gronau, S. Sharma, & G. Canals (Eds.) Springer.
- Almalki, M., Fitzgerald, G., & Clark, M. (2011). Health care system in Saudi Arabia: An overview. *Eastern Mediterranean Health Journal*, 17(10).
- All internet security. (2015). From SecureCode to Facial Recognition with MasterCard Authentication. Retrieved from: <http://www.all-internet-security.com/from-securecode-to-facial-recognition-with-mastercard-authentication/>
- Al-Saggaf, Y. (2004). The effect of online community on offline community in Saudi Arabia. *The Electronic Journal of Information Systems in Developing Countries*, 16.
- Al-Saggaf, Y., & Williamson, K. (2004). Online communities in Saudi Arabia: Evaluating the impact on culture through online semi-structured interviews. Paper presented at the Forum Qualitative Sozialforschung/Forum: Qualitative Social Research.
- American Hospital Association. (2010). The road to meaningful use: What it takes to implement electronic health record systems in hospitals. Trendwatch: American Hospital Association.
- American Medical Association. (1999). *Cultural competence compendium*. American Medical Association.
- Arab News. (2014, March 21). World's largest biometric centre planned. Retrieved from: <http://www.arabnews.com/news/543586>

- Aziz, R. (2011). Hijab–The Islamic Dress Code: Its historical development, evidence from sacred sources and views of selected muslim scholars.
- Bhattacharyya, D., Ranjan, R., Farkhod Alisherov, A., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3), 13-28.
- Bickford, C. J., & Hunter, K. M. (2006). Theories, models, and frameworks. *Essentials of nursing informatics*, 89-106. New York: McGraw-Hill
- Bieber, E. J., Richards, F., & Walker, J. M. (2005). *Implementing an electronic health record system*. J. M. Walker, E. J. Beiber, R. Richards, & S. Buckley (Eds.) London: Springer-Verlag.
- Blumenthal, D., & Tavenner, M. (2010). The “meaningful use” regulation for electronic health records. *New England Journal of Medicine*, 363(6), 501-504.
- Bolle, R. M., Connell, J., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics*. New York: Springer-Verlag.
- Boonstra, A., Versluis, A., & Vos, J. F. (2014). Implementing electronic health records in hospitals: A systematic literature review. *BMC health services research*, 14(1), 1.
- Bryman, A., & Bell, E. (2015). *Business research methods*. Oxford University Press, USA.
- Choudhary, D., Tiwari, S., & Singh, A. K. (2012). A survey: Feature extraction methods for iris recognition. *International Journal of Electronics Communication and Computer Technology*, 2(6), 275-279.
- Cohen, J., & Ezer, T. (2013). Human rights in patient care: A theoretical and practical framework. *Health and Human Rights Journal*, 15(2).
- Creative Research Systems (2012). *Sample size calculator*. Retrieved from: <http://www.surveysystem.com/sscalc.htm>
- De Bord, J., Burke, W., & Dudzinski, D.M. (2013). Confidentiality. *Ethics in Medicine*. University of Washington School of Medicine. Retrieved From: <https://depts.washington.edu/bioethx/topics/confiden.html>
- Delac, K., & Grgic, M. (2004). A survey of biometric recognition methods. In Electronics in Marine, 2004. Proceedings from *Elmar 2004. 46th International Symposium* (pp. 184-193). IEEE.
- Díaz-Palacios, J. R., Romo-Aledo, V. J., & Chinaei, A. H. (2013, March). Biometric access control for e-health records in pre-hospital care. In Proceedings of the Joint EDBT/ICDT 2013 Workshops (pp. 169-173). ACM.
- Du, Y. E. (2013). *Biometrics: From fiction to practice*. Hoboken: CRC Press.

- Fink, A. (2009). *How to Conduct Surveys*. Thousand Oak: Sage.
- Galanti, G.-A. (2004). *Caring for patients from different cultures*: University of Pennsylvania Press.
- Gostin, L. O., Levit, L. A., & Nass, S. J. (2009). *Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research*. Washington DC: National Academies Press.
- Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, 80(2), e26-e31.
- Hembroff, G. C., Wang, X., & Muftic, S. (2011). Providing an additional factor for patient identification based on digital fingerprint. In *Proceedings of the 2nd USENIX conference on Health security and privacy* (pp. 7-7). USENIX Association.
- Hoerbst, A., & Ammenwerth, E. (2010). Electronic health records. A systematic review on quality requirements. *Methods Inf Med*, 49(4), 320-336.
- Hone, K., & Eloff, J. (2002). What makes an effective information security policy? *Policy Network Security*, 20(6), 14-16.
- Huebler, F., & Lu, W. (2013). Adult and youth literacy: National, regional and global trends, 1985-2015. Montreal, QC: UNESCO Institute for Statistics.
- Hustinx, P. (2010). European Data Protection Supervisor. In Third Joint Parliamentary Meeting on Security: Which technologies and for what security (pp. 2001-2002).
- Iacona, A. (2014). Health care information technology: Securing the electronic health record with biometric technology. Undergraduate Review. *A Journal of Undergraduate Student Research*, 15(1), 4-8.
- International Medical Informatics Association. (2001). A code of ethics for health informatics professionals. *J Inst Health Rec Inf Manag*, 42, 27-31.
- ISO/IEC, (2005). Information technology – code of practice for information security management, ISO/IEC 27002:2005. The International Organization for Standardization/The International Electro-technical Commission.
- Jackson, S. (2014). *Research methods: A modular approach (3rd ed.)*. Cengage Learning.
- Jaeger, P. T. (2007). Information policy, information access, and democratic participation: The national and international implications of the Bush administration's information politics. *Government Information Quarterly*, 24(4), 840-859.
- Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *Information Forensics and Security, IEEE Transactions on*, 1(2), 125-143.

- Jaiswal, S., Bhadauria, S. S., & Jadon, R. S. (2011). Biometric: Case study. *Journal of Global Research in Computer Science*, 2(10), 19-48.
- KFSH. (2015). *Departments*. Retrieved from: http://www.kfsh.med.sa/KFSH_Website/KFSHDefault.aspx?DT=D&T=30
- Klokoza, A. (2010). *Comparison of various biometric methods*. Southampton, UK: Electronic and Computer Science University of Southampton.
- Krawczyk, S., & Jain, A. K. (2005). Securing electronic medical records using biometric authentication. Paper presented at the Audio-and Video-Based Biometric Person Authentication.
- Kwon, J., & Johnson, M. E. (2014). Meaningful Healthcare Security: Does “Meaningful-Use” Attestation Improve Information Security Performance? Paper presented at the Workshop on the Economics of Information Security (WEIS), Penn State University.
- Le, C., & Jain, R. (2009). *A survey of biometrics security systems*. St Louis: Washington.
- Lorenzi, N. M., Kouroubali, A., Detmer, D. E., & Bloomrosen, M. (2009). How to successfully select and implement electronic health records (EHR) in small ambulatory practice settings. *BMC medical informatics and decision making*, 9(1), 15.
- Macintyre, N. R., & Galvin, W. F. (2015). *Respiratory care: Principles and practice*. Jones & Bartlett Publishers.
- Mahmoud, M. S. A. (2015). Designing and Implementing of Electronic Health Record System in KSA Using SQL & Asp. *Net. Journal of Medical Biomedical and Applied Sciences*, 2(9), 01-12.
- Mahnken, S. (2014). Today's authentication options: The need for adaptive multifactor authentication. *Biometric Technology Today*, 2014(7), 8-10.
- Marohn, D. (2006). Biometrics in healthcare. *Biometric Technology Today*, 14(9), 9-11.
- Mathers, N., Fox, N. J., & Hunn, A. (1998). *Surveys and questionnaires*. NHS Executive, Trent.
- Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging 2002* (pp. 275-289). International Society for Optics and Photonics.
- McCallister, E., Grance, T., & Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). DIANE Publishing, Darby, PA, US
- Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Manag Healthc Policy*, 4, 47-55.
- Mittestaedt, J., Shafy, S. (2015, June 23). Lifting the Veil: How Working Women Are Remaking Saudi Arabia. Retrieved from:

<http://www.spiegel.de/international/world/more-saudi-arabia-women-working-despite-limited-rights-a-1040135.html>

- Okoh, E., & Awad, A. I. (2015). Biometrics applications in e-health security: A preliminary survey. In *Health Information Science* (pp. 92-103). Springer International Publishing.
- Omotosho, A., Adegbola, O., Adelakin, B., Adelakun, A., & Emuoyibofarhe, J. (2015). Exploiting multimodal biometrics in e-privacy scheme for electronic health records. *JBAH*, 18. Retrieved from: *arXiv preprint arXiv:1502.01233*.
- Oxford Dictionary. (2015). Islam. Retrieved from: <http://www.oxforddictionaries.com/definition/english/islam>
- Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, 6(2), 73.
- Perrin, R. A. (2002). Biometrics technology adds innovation to healthcare organization security systems.(Digital Perspectives). *Healthcare Financial Management*, 56(3), 86-89.
- Peltier, T. R. (2004). Information security policies and procedures: A practitioner's reference. London: Auerbach Publications.
- Preece, J., Rogers, Y., & Sharp, H. (2002). Interaction Design: Beyond Human-Computer Interaction. John Wiley & Sons Inc.
- Ramli, S. N., Ahmad, R., Abdollah, M. F., & Dutkiewicz, E. (2013). A biometric-based security for data authentication in wireless body area network (wban). Paper presented at the Advanced Communication Technology (ICACT), 2013 15th International Conference on.
- Ranade-Kharkar, P., Pollock, S. E., Mann, D. K., & Thornton, S. N. (2014). Improving Clinical Data Integrity by using Data Adjudication Techniques for Data Received through a Health Information Exchange (HIE). Paper presented at the AMIA Annual Symposium Proceedings.
- Rezaeibagha, F. (2013). Privacy and Data Security of Electronic Patient Records (EPR) Sharing Case studies: Iran and Sweden. A thesis presented in partial fulfilment of the requirements of Degree of Master of Science in Information Security at Lulea University of Technology.
- RightPatient. (2015). *Why Experience Matters When Selecting a Biometric Patient Identification Solution*. Retrieved from: <http://www.rightpatient.com/blog/why-experience-matters-when-selecting-a-biometric-patient-identification-solution/>
- Ross, A. A., Shah, J., & Jain, A. K. (2005). *Toward reconstructing fingerprints from minutiae points*. In *Defense and Security* (pp. 68-80). International Society for Optics and Photonics.
- Rowe, R. K. (2005). A multispectral sensor for fingerprint spoof detection. *Sensors*, 22(1), 25-27.

- Rowe, R., Nixon, K., & Butler, P. (2008). Multispectral fingerprint image acquisition. *Advances in biometrics*, 3-23.
- Ruiz-Blondet, M., Khalifian, N., Armstrong, B. C., Jin, Z., Kurtz, K. J., & Laszlo, S. (2014). Brainprint: Identifying unique features of neural activity with machine learning. In *Proc. 36th Annual Conf. of the Cognitive Science Society*.
- Saini, R., & Rana, N. A. (2014). Hybrid Framework of Facial Expression Recognition using SVD & PCA. *International Journal of Computer Science and Information Technologies*, 5(5).
- Schnapp, J. T., & Michaels, A. (2012). *The electric information age book*. NY: Princeton Architectural.
- Simon, S., Evans, J. S., Benjamin, A., Delano, D., & Bates, D. (2009). Patients' attitudes toward electronic health information exchange: Qualitative study. *Journal of Medical Internet Research*, 11(3), e30.
- Silow-Carroll, S., Edwards, J. N., & Rodin, D. (2012). Using electronic health records to improve quality and efficiency: The experiences of leading hospitals. *Issue Brief (Common Fund)*, 17, 1-40.
- Spence, B. (2011, November 4). Hospitals can finally put a finger on biometrics. Retrieved from: <http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-finger-on-biometrics>
- Spitz, G., Niles, F. L., & Adler, T. J. (2006). Web-based survey techniques (Vol. 69). Transportation Research Board.
- Statistics How To (2015). *How to get a stratified random sample in statistics*. Retrieved from: <http://www.statisticshowto.com/stratified-random-sample/>
- Trader, J. (2012). Biometric patient id technology: Is it the future of patient access? *Insightful Coverage of Health Care Innovation*. Retrived from: <http://www.hitconsultant.net/2012/10/18/biometric-patient-id-technology-is-it-the-future-of-patient-access>
- True, T. (2012). Voice biometrics, the key to simple and secure access to health information. Retrieved from: <http://www.beckershospitalreview.com/healthcare-information-technology/voice-biometrics-the-key-to-simple-and-secure-access-to-health-information.html>
- Ultra Electronics. (2015). Ultra secure proximity. Retrieved from: <http://ultraid.com/smart-cards/125-khz-proximity/>
- U.S. Department of Health and Human Services. (2001). *National standards for culturally and linguistically appropriate services in health care: Final report*. Washington, DC: U.S. Department of Health and Human Services, Office of Minority Health.

- Vogel, F. E. (2000). *Islamic Law and the Legal System of Saudi Arabia* (Vol. 8): Boston: Brill Academic Pub.
- Waegemann, P. (2003). EHR vs. CPR vs. EMR. Retrieved from <http://www.healthcare-informatics.com>
- Wainer, J., Campos, C. J. R., Salinas, M. D. U., & Sigulem, D. (2008). Security requirements for a lifelong electronic health record system: An opinion. *The Open Medical Informatics Journal*, 2, 160.
- Walker, D.-M. (2014). *An Introduction to Health Services Research: A Practical Guide*. Los Angeles: Sage.
- Wang, Y., Hu, J., & Phillips, D. (2007). A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 573-585.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193-220.
- Whither Biometrics Committee. (2010). *Biometric Recognition: Challenges and Opportunities*. Doi: 10.17226/12720
- Zandieh, S., Yoon-Flannery, K., Kuperman, G., Langsam, D., Hyman, D., & Kaushal, R. (2008). Challenges to EHR implementation in electronic-versus paper-based office practices. *Journal of General Internal Medicine*, 23(6): 755–761.
- Zhang, D. D. (2013). *Automated biometrics: Technologies and systems* (Vol. 7). New York: Springer US.
- Zhao, W., Krishnaswamy, A., Chellappa, R., Swets, D. L., & Weng, J. (1998). Discriminant analysis of principal components for face recognition. In: *Face Recognition* (pp. 73-85). Berlin: Springer.
- Zuniga, A. E. F., Win, K. T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of Medical Systems*, 34(5), 975-983.

Appendix A: Covering letter and questionnaire

Dear doctors, managers and IT professionals at King Fahad Specialist Hospital,

I am a student from Massey University, Auckland, New Zealand, studying towards a Masters in Information Science. I am conducting a survey for my thesis. The thesis is titled “EHRs at King Fahad Specialist Hospital: an overview of professionals’ perspectives on the use of biometric patient identification for privacy and confidentiality taking into consideration culture and religion” and is under the direction of my supervisor Dr. Kuda Dube, who can be reached through K.Dube@massey.ac.nz , telephone: +64 (06) 356 9099 ext. 84145.

The objectives of this research are as follows:

1. To establish whether you recommend non-biometric mechanism or a Biometric Patient Identification mechanism (BPI) to access Electronic Health Records (EHRs) and which subtypes of these two you recommend.
2. Analyse your views of which type(s) of BPI mechanism you recommend, if any, for both Saudi males and females patients: fingerprints; face recognition; iris recognition; voice pattern, and/or hand-palm veins.
3. To determine your level of awareness and commitment to EHR privacy, confidentiality, and policy (if any policy exists) in the Saudi Arabian cultural and religious context.

Biometric Patient Identification (BPI) is a revolutionary technology that is used to identify patients through their unique or distinctive physiological features such as fingerprints, face, eyes, and voice to enable staff to access Electronic Health Records (EHRs). BPI involves the scanning of the relevant body part; for example the facial recognition technology requires the face of the patient to be uncovered so it can be scanned by scanning device and the iris technology requires the eyes to be scanned, as do the fingerprints. Similarly, hand-palm veins requires the scanning of the palm and voice recognition requires patients to speak through a speaker to identify the voice prints of individual patients.

Participation in the survey is entirely voluntary and there are no known or anticipated risks associated with participation in the survey. All information provided by you will be kept strictly confidential and will only be used for academic purposes.

Please note that this project has been evaluated by peer review and judged to be low risk. Consequently, it has not been reviewed by one of the University’s Human Ethics Committees. The researcher(s) named above are responsible for the ethical conduct of this research.

If you have any concerns about the conduct of this research that you wish to raise with someone other than the researcher(s), please contact Dr Brian Finch, Director, Research Ethics, telephone: +64 (6) 356 9099 ext 86015, email: humanethics@massey.ac.nz

The survey should take around 5-10 minutes to complete. Your participation is highly appreciated.

Adel Khawaji
Massey University
Email: adel.khawaji@hotmail.com

Section A

This section provides background information of the participants who took part in the survey. This section will also stratify the participants based on their professional roles in King Fahad Specialist hospital.

What is your profession in the hospital? *

Please choose **only one** of the following:

- ☐ Doctor
- ☐ Manager
- ☐ IT Professional

Are you a Saudi citizen? *

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

How long have you been working in health care? *

Please choose **only one** of the following:

- ☐ 6 months or less
- ☐ more than 6 months but less than 2 years
- ☐ 2 years or more

How long have you been using electronic health records (EHRs)? *

Please choose **only one** of the following:

- ☐ 6 months or less
- ☐ more than 6 months but less than 2 years
- ☐ 2 years or more

Section B

This section explores the paradigms of data storage through the EHR systems in the hospital and will also help to determine the processes that are in place to ensure the safety and integrity of the patient data. This section will also explore the data access restrictions that are in place and the different reasons for accessing patient's EHR.

Does your hospital store patient records electronically? *

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

How much access do you have to Electronic Health Records (EHRs)? *

Please choose **only one** of the following:

- ☐ Full access
- ☐ Limited access
- ☐ No access

In your opinion, what is the main reason of accessing EHRs? *

Please choose **all** that apply:

- ☐ My job
- ☐ Favour for a friend/family

Section C

This section fundamentally explores the current methods of accessing patient records. The section will also help identify the biometric and non-biometric methods that are being used in the hospital to access electronic health records.

Usually, what type of method is used to access EHRs in the hospital? *

Please choose **all** that apply:

- ☐ Biometrics
- ☐ Non-biometrics
- ☐ Other

What biometric tool(s) are used in the hospital? *

Please choose **all** that apply:

- ☐ Fingerprints
- ☐ Face recognition
- ☐ Iris recognition
- ☐ Voice pattern
- ☐ Hand-palm veins
- ☐ Not applicable
- ☐ Other

What non-biometric tool(s) are used in the hospital *

Please choose **all** that apply:

- ☐ Password
- ☐ Tokens
- ☐ Proximity card
- ☐ Not applicable
- ☐ Other

Section D

This section explores your point of view about biometric patient identification and non-biometrics methods. Your answers will assist in determining your perception or believes on the effectiveness of the biometric patient identification systems over non-biometric systems with regard to safeguarding EHRs. This section will also ask you questions relevant to any possible influence of culture and religion on biometric patient identification technology.

To what extent do you agree with the following statements: *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Biometric patient identification systems provide more security to EHRs.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In hospitals, biometric patient identification systems would be more preferable than non-biometric systems.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Biometric patient identification systems are more efficient than paper-based systems.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Culture would have an impact on the use of biometric technologies that utilise body feature(s) of patients in hospital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Religion would have an impact on the use of biometric technologies that utilise body feature(s) of patients in the hospital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

In your opinion, what type of biometric system(s) would be suitable for Saudi male patients in the hospital? *

Please choose **all** that apply:

- ☐ Fingerprints
- ☐ Face recognition
- ☐ Iris recognition
- ☐ Voice pattern
- ☐ Hand-palm veins
- ☐ I do not know

In your opinion, what type of biometric system(s) would be suitable for Saudi female patients in the hospital? *

Please choose **all** that apply:

- ☐ Fingerprints
- ☐ Face recognition
- ☐ Iris recognition
- ☐ Voice pattern
- ☐ Hand-palm veins
- ☐ I do not know

Section E

This section explores security and the policy of accessing patients' records. The questions will help determine if the EHR users are fully aware of the risks that are involved in the handling of patient record. The focus is also on the security policies that are implemented in the hospital to safeguard patient health data and if all the hospital's professionals are aware of the same.

Have you been given any EHR security policy document? *

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

Do you believe that the EHR security policy protects the privacy of EHRs efficiently? *

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

Do you believe that the EHR security policy protects the c of EHRs efficiently? *

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

To what extent do you agree with the following statements: *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Neither agree disagree	nor Agree	Strongly agree
The EHR security policy procedures are fully understandable among staff.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EHRs can be revealed to any of the patient's family without the patient's consent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EHRs can be revealed to any of the patient's friends without the patient's consent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Section F

This section is designed to understand staff's commitment to and understanding of cultural and religious issues in relation to EHR's privacy and confidentiality.

To what extent do you agree with the following statements: *

Please choose the appropriate response for each item:


	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Cultural issues have a great impact on EHR privacy and confidentiality.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Religious issues have a great impact on EHR privacy and confidentiality.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health staff are fully committed and responsible for protecting patients' privacy and confidentiality.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Saudi patients take cultural issues related to their privacy and confidentiality very seriously.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Saudi patients take religious	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly agree
issues related to their privacy and confidentiality very seriously.					
Revealing a patient's EHR to a family member without patient consent may expose patient's life to danger.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Submit your survey.

Thank you for completing this survey.

This email was sent to the managing director of KFSH for seeking permission.



RE: Permission 

From: A Khawaji [adel.khawaji@hotmail.com]
Sent: Thursday, August 20, 2015 9:53 AM
To: Academic & T Dep. [eptm@kfsh.med.sa]
Subject: Permission

To: The managing director of King Fahad Specialist Hospital
Dear Sir/Madam:

I am student from Massey University, Auckland New Zealand studying towards a Masters degree in information Science. I am conducting a survey for a thesis. The thesis is titled (Ensuring Privacy and Confidentiality Based on Religion and Culture in King Fahad Specialist Hospital) and is under the direction of my supervisor Dr. Kuda Dube, who can be reached through K.Dube@massey.ac.nz Telephone: +64 (06) 356 9099 ext. 84145

Participation in the survey is entirely voluntary and there are no known or anticipated risks associated with participation in the survey. The sought survey participants are physicians, managers and IT professionals working in King Fahad Specialist Hospital. All information provided by the participants would be kept on extreme confidentiality and would be used for academic purposes only.

Please note that this project has been evaluated by peer review and judged to be low risk. Consequently, it has not been reviewed by one of the University's Human Ethics Committees. The researcher(s) named above are responsible for the ethical conduct of this research.

If you have any concerns about the conduct of this research that you wish to raise with someone other than the researcher(s), please contact Dr Brian Finch, Director, Research Ethics, telephone +64 (06) 356 9099 extn 86015, email humanethics@massey.ac.nz.

The survey will only take 5-10 minutes to complete. Please click on the hyperlink below to view the survey and obtain background information on it:
<http://bit.ly/1g4SMYf>

I respectfully seek your permission and approval to conduct this study. Please feel free to communicate with me regarding the study.

Thanking you in advance for your assistance.


Sincerely,

Adel Khwaji
adel.khawaji@hotmail.com
+64 210 252 9860


The reply from the management director of KFSH



RE: Permission 




Academic and Training Department
To: A Khawaji



Dear Adel Khwaji,

Your request has been approved and the survey link has been emailed to the managers, IT staff and Physicians accordingly.

Best Regards.



King Fahad Specialist Hospital-Dammam
Academic and Training Department
Phone +966138442222 Ext. 1140
Email eptm@kfsh.med.sa
www.kfsh.med.sa

From: A Khawaji [adel.khawaji@hotmail.com]
Sent: Thursday, August 20, 2015 9:53 AM
To: Academic & T Dep. [eptm@kfsh.med.sa]
Subject: Permission

To: The managing director of King Fahad Specialist Hospital
Dear Sir/Madam:

Appendix B: Ethics approval received from MUHEC



MASSEY UNIVERSITY ALBANY

18 August 2015

Adel Khwaji
A26/210 Dairy Flat Highway
Albany
North Shore 0632

Dear Adel

Re: EHRs: Ensuring Privacy and Confidentiality Based on Culture and Religion in Saudi Arabia

Thank you for your Low Risk Notification which was received on 13 August 2015.

Your project has been recorded on the Low Risk Database which is reported in the Annual Report of the Massey University Human Ethics Committees.

You are reminded that staff researchers and supervisors are fully responsible for ensuring that the information in the low risk notification has met the requirements and guidelines for submission of a low risk notification.

The low risk notification for this project is valid for a maximum of three years.

Please notify me if situations subsequently occur which cause you to reconsider your initial ethical analysis that it is safe to proceed without approval by one of the University's Human Ethics Committees.

Please note that travel undertaken by students must be approved by the supervisor and the relevant Pro Vice-Chancellor and be in accordance with the Policy and Procedures for Course-Related Student Travel Overseas. In addition, the supervisor must advise the University's Insurance Officer.

A reminder to include the following statement on all public documents:

"This project has been evaluated by peer review and judged to be low risk. Consequently, it has not been reviewed by one of the University's Human Ethics Committees. The researcher(s) named above are responsible for the ethical conduct of this research."

If you have any concerns about the conduct of this research that you wish to raise with someone other than the researcher(s), please contact Dr Brian Finch, Director (Research Ethics), telephone 06 356 9099, extn 86015, e-mail humanethics@massey.ac.nz."

Please note that if a sponsoring organisation, funding authority or a journal in which you wish to publish requires evidence of committee approval (with an approval number), you will have to provide a full application to one of the University's Human Ethics Committees. You should also note that such an approval can only be provided prior to the commencement of the research.

Yours sincerely

Brian T Finch (Dr)
Chair, Human Ethics Chairs' Committee and
Director (Research Ethics)

cc **Dr Kuda Dube**
School of Engineering and Advanced Technology
Palmerston North campus

Professor Don Cleland
Head Of School of Engineering and Advanced
Technology
Palmerston North campus

Massey University Human Ethics Committee
Accredited by the Health Research Council

Approval of title modification from MUHEC

