Article type: Review Article

Usable security in Electronic Health Record System: A review on the Saudi Arabian perspective

Samina A. Khan[1,2] Syaheerah L. Lutfi[1,*]

[1] School of Computer Sciences, Universiti Sains Malaysia, 11800 Gelugor, Pulau, Penang, Malaysia

[2] Department of Medical Education, Medical Informatics and E-Learning Unit, College of Medicine, King Saud University, Riyadh, Saudi Arabia

***Corresponding Author**

Dr. Syaheerah L. Lutfi

School of Computer Sciences Universiti Sains Malaysia, Pulau Penang, MY

Email: syaheerah@usm.my

Abstract:

Background and objective: The electronic health record (EHR) is the fundamental building block of digital healthcare. With the increase of sensitive personal data stored in the EHR, the usability of the system and information security become important concerns. Experts are constantly developing techniques to improve security while maintaining usability. This is where usable security comes into play. More specifically, it is the prevention of unauthorized access while maintaining simplicity for the user. This review paper analyses the available evidence on security and usability of healthcare software to derive recommendations for the Saudi healthcare sector.**Method:**A review of the current literature was conducted using PubMed, Google Scholar, and the results were analysed.**Results:**Healthcare professionals work under time pressure and with limited resources. They need efficient and usable digital tools that include security measures. Lack of certainty undermines information security and ultimately compromises patient safety. There are no clear global guidelines for usable security in healthcare. Usability research in other fields suggests that such research would need to be specific to a country or a region with shared cultural and linguistic traits.

Conclusion: The influence of usability in health care, and EHR security in particular, shouldbe empirically investigated in a Saudi Arabian context in future studies.

Keywords: Cyber-security; Electronic Health Records; Hospital Information Systems; Information security; Usability; Usable security; Saudi Arabia

1. Introduction

Digital healthcare is a highly dynamic field with a high rate of innovation, and the recent pandemic has further accelerated digitization(Alshamrani, 2021; Horgan et al., 2020; Kaplan, 2020). Improved accessibility of information is one of the key benefits of digitalization in healthcare(Everson & Butler, 2020). However, it is also an area that requires conscientious use of technology more than any other industry(Thimbleby, 2013). Patients' most private data

are at stake. Therefore, the security and privacy of patient data has always been one of the most critical issues in digital healthcare(Martin, Kinross, & Hankin, 2017). Patient trust is an essential factor in the relationship between patients and healthcare professionals, which is essential for successful treatment. Security measures in healthcare IT must therefore also contribute to the perceived safety of patients. Physical protection mechanisms in healthcare IT and patients' perceived information security do not necessarily correlate(Peikari, T, Shah, & Lo, 2018). As technology becomes more prevalent in healthcare, its usability becomes increasingly important to healthcare professionals, patients, and other stakeholders(Alotaibi & Federico, 2017). Given limited time and human resources, technologies must be easy to use without the need for extensive training(Powell-Cope, Nelson, & Patterson, 2008). With heterogeneous patient populations that are not exclusively "digital natives," ease of use is essential(Alessa, S Hawley, Alsulamy, & de Witte, 2021). How to reliably assess and compare the usability of healthcare information systems is the subject of much research and debate. Conceivable approaches include the Think Aloud (TA) and Heuristic Evaluation (HE) methods. These methods are suitable for a specific subset of usability problems; TA for effectiveness and efficiency, HE for satisfaction, learnability and error prevention(Khajouei & Farahani, 2020). However, in an increasingly connected and digital world of healthcare, the increased use of technology(Sohaib, Naderpour, Hussain, & Martinez, 2019), cybersecurity of IT(Kaur & Ramkumar, 2021), and medical technology have also led to an unprecedented increase in the incidence of data breaches and data theft(Sahu & Pandey, 2015). This has raised concerns that systems will have to keep up with an increase in attack vectors("Healthcare Cybersecurity-HIPPA Journal," 2021).

However, secure systems tend to be less user-friendly because additional security measures impose more effort and mental load on the user(A. Jøsang, AlFayyadh, Grandison, AlZomai, & McNamara, 2007). Practitioners are continuously working on various solutions and techniques to enhance the security of software while ensuring usability(Al-Zahrani, 2020). This makes the development of the field of "Usable Security" more urgent than ever. Usable security means designing secure systems while minimizing usability(Ka-Ping, 2004; Kainda, Fléchais, & Roscoe, 2010). Also defined as "the notion that security tools and measures must satisfy usability requirements in order to function as intended"(Das, Dingman, & Camp, 2018). Many studies have been conducted to study usable security over healthcare systems; however, to the best of our knowledge, there has been no review article that has studied the state of usable security in the context of Saudi Arabian healthcare systems. Therefore, this article aims to better understand the topic of usable security and identify the current state-of-the art in healthcare, specifically in the Arab world and with a greater focus on Saudi Arabia.

2. Methodology

The authors conducted a literature search (year range: 2000 - 2020) in PubMed (MEDLINE) and Google Scholar to identify studies that address usability in computer security, invisible and user-centered security, electronic health record (EHR) security in general and specifically in the Arab region, and usability in health security. These areas were chosen to approach the topic of usable security in healthcare in Saudi Arabia from different directions after an initial search showed that literature on usability in healthcare in Saudi Arabia or other Arab

countries is virtually non-existent. For the search, we used the following keyword combinations and permutations to identify relevant publications in the databases:

- Security, healthcare, hospital, electronic health records, electronic patient records, electronic medical records
- Usable security, invisible security, user-centered security, user-friendly security, usability and security, trade-off between usability and security.
- Information security, data protection, patient safety, malware, ransomware, cyber attack
- Saudi Arabia, Arabic countries, Arabic language, usability, computer systems, culture-specific usability

To illustrate EHR security and current threats, the scientific database search was supplemented with a Google search for the keywords "ransomware", "hospitals",2020" and "2021" as these very recent incidents have not yet been reflected in the scientific literature. Exclusion criteria were publications before 2010 for articles focusing on specific technologies, as these are now outdated. For articles dealing with cultural and general usability aspects unrelated to specific technologies, the age of the publication was not an exclusion criterion, as their results are less likely to be outdated. The second exclusion criterion was publication in a language other than English. Finally, publications were excluded if they covered research questions already addressed by another included paper that was more comprehensive or recent; in other words, if multiple papers from a research group or different research groups addressed the same or a similar topic with similar results, only the most recent or comprehensive paper was included. Of each paper that met the inclusion criteria, the authors also evaluated its reference section for other related publications.

3. Results

After filtering publications that met the exclusion criteria, 36 publications were identified and included in this review. As expected, there were no articles that directly addressed or made recommendations on the state of usable security in healthcare Saudi Arabian. However, there were several included publications for each of the relevant topics listed above (ranging from usability in computer security, invisible and user-centered security, EHR security, and usability in healthcare security.

4. Discussion

4.1 Usability, Security, and Usable Security

CIA (Confidentiality, Integrity, and Availability) defines usability as "the degree or level to which specific users can use a product to achieve specific goals with efficiency, effectiveness, and satisfaction" (Bai et al., 2016). In addition, security is the way of proceeding in an organization regarding information security in order to protect information assets and influence system usability(Abd-El-Barr, 2021), and security behavior of employees(AlHogail & Mirza, 2014). Traditionally, the security and usability of a system have been considered antagonistic to each other(Garfinkel & Lipford, 2014)in the sense that usability and convenience must be weighed against increased security. For example, clinicians and other

medical staff have traditionally preferred single sign-on (SSO) systems over more secure multi-factor authentication schemes(James, Marwaha, Brough, & John, 2020). However, it is increasingly recognized that usability is a necessary requirement for any truly secure system. Security measures with suboptimal usability lead to reluctant user behavior that ignores or even intentionally bypasses these measures(Garfinkel & Lipford, 2014). Furthermore, studies have shown that poor usability leads to poor security(Whitten & Tygar, 1999). The principles of usable security were introduced to the cybersecurity community as early as 1975. They recognize the importance and influence of usability in terms of security and acceptance of interactive systems between humans and computers(Saltzer & Schroeder, 1975). However, they are still far from being continuously applied in all industries(Theofanos, 2020), as security professionals either did not recognize the importance or lacked the expertise to consider and address potential usability issues(Cranor & Garfinkel, 2005). Fortunately, the research community has agreed for more than a decade that a system must be useful to be secure, i.e., develop secure systems that people can use. Since then, the usable security community has worked hard to balance usability and security, e.g., i) user interfaces to increase security awareness, ii) 2-factor authentication systems(Storer et al., 2013), iii) effective anti-phishing software(Herzberg & Margulies, 2013). Therefore, security focuses on preventing unauthorization, while usability refers to the ease with which users use the "easy to keep" software formula(Sahu, Pandey, & Kumar, 2014).Therefore, usable security must be the main goal of focus in IT industries. In an ideal world, security measures would be invisible to the end user. This paradigm is known as invisible security and would be most helpful in industries where resources, especially manpower and time, are scarce, such as healthcare(Dykstra, 2020). To date, there is no overarching system for invisible security in any industry. Instead, it has been implemented in a modular and patchwork fashion across different platforms and modules, such as automatic updates of operating systems and applications(Theofanos, 2020). A defining feature of digital healthcare, especially telemedicine, is the reduction of face-to-face interaction of patients with physicians and other professionals. This is not an undesirable effect per se, as it contributes to the effectiveness of healthcare delivery, e.g., by allowing patients to stay at home while seeking medical advice, either because they are immobile, live in a remote or underserved area, want to avoid situations where infectious diseases could be transmitted, or for other reasons(Bradford, Caffery, & Smith, 2016). However, the elimination of real human contact requires patients to place their trust in technology rather than human actors, which is counterintuitive for a large portion of the patient population. Furthermore, as digital health services become more accessible and widespread in the population, a significant proportion of users do not have much prior knowledge of digital systems and therefore cannot be expected to behave like the perfect (or perfectly safe) user(Issa, Murray, & Ernst, 2018). One way to address this novel challenge is through a paradigm known as user-centered security(Vega-Barbas, Seoane, &Pau, 2019), which specifically considers users' fears and expectations. Proponents of user-centric security view this concept as an evolved version of usable security. It not only revises conventional security mechanisms to make them more user-friendly, but also puts the user at the center of the design and development of secure systems from the beginning(Smetters & Grinter, 2002; Vega-Barbas et al., 2019). Therefore, user-centric security in healthcare and other contexts has two goals: First, to enable users to use systems securely without prior

knowledge of information security or even without significant prior experience IT. Second, to enable users to be aware of and confident in the security of the transactions they perform(Vega-Barbas et al., 2019). (See Table 1)

Security Terms	**Definitions**
1. Security	Security of information or information systems regardless of domain(Security, 2019).
2. Usable Security	Secure information system built with a human-centred focus(Lennartsson, Kävrestad, & Nohlberg, 2020).
3. Invisible Security	A paradigm of cybersecurity protections that do not require end-user attention or action(Dykstra & Spafford, 2018).
4. User-Centred security	Security systems that have usability as a primary goal, adequately support the user in the use of services, provide guarantees related to system operation, and are compatible with applicable laws, norms, and ethical standards(Vega-Barbas et al., 2019; Zurko, 2005; Zurko & Simon, 1996).

Table 1 Security, Invisible Security, Usable Security, and User-centred security

4.2 Security ofthe EHRs

A key component of digital health is the electronic health record (EHR) or electronic medical record (EMR). Here, all the key goals of information security come into play: availability is needed for rapid diagnosis and treatment, integrity for correct medical decisions, and confidentiality to protect patient rights(Ganiga, Pai , Pai, & Sinha, 2020). In recent years, healthcare has increasingly been targeted by malicious agents. Even though hospitals and other facilities are generally not a source of valuable industrial data that invite industrial espionage, attackers still monetize the data in various ways(Ibarra, Jahankhani, & Kendzierskyj, 2019) . One of the most prominent attack vectors on hospitals in general and EHRs over the past five years has been ransomware. This type of malware encrypts data and offers the decryption keys in exchange for a ransom, usually paid in Bitcoin or another digital and potentially anonymous currency(Collier, 2017; Spence , Paul III, & Coustasse, 2017). As recently as the fall of 2020, a ransomware attack on a hospital in Duesseldorf resulted in one death(Yeng, Fauzi, & Yang, 2020). So far, there are no known ransomware attacks on Saudi hospitals. Of course, since there is no guarantee that the decryption keys will be released once the ransom is paid, authorities around the world typically recommend not paying the ransom and instead attempting to restore the facility to normal operations by recovering the data from backups as quickly as possible. This, of course, requires a solid backup strategy before a ransomware attack takes place(Kelpsas & Nelson, 2016). Other defenses against ransomware attacks are essentially congruent with defenses against malware: rapid updates to all systems, intrusion detection and prevention systems including firewall and antivirus software, and security-conscious employees (not just IT). They are necessary, but holistic rather than specific to EHR protection. EHR-specific security measures are predominantly in the hands of EHR vendors. Reliable encryption of patient data during storage and transmission is critical

for health information security, as the main protocols used in healthcare information processing - HL7 and FHIR - focus on interoperability rather than security(Saripalle, Runyan, & Russell, 2019) and therefore do not include cryptographic measures.

4.5 EHR and Healthcare Information Security in the Arab World

In 2020, an Egyptian team of researchers reviewed privacy and security issues, focusing on EHRs (Keshta & Odeh, 2020). They divided security issues surrounding EHR into administrative, physical and technical themes. Administrative safeguards include auditing, the appointment of a dedicated security officer, and contingency planning. Physical safeguards include physical barriers to software and hardware access and the assignment of security roles. Finally, Technical safeguards include encryption, firewalls and antivirus software. The authors emphasized the role of multidisciplinary efforts in managing the privacy and security of EHR, including collaboration between IT and telecommunications and the medical departments of the hospital. While this review presents security and privacy in a normative way, a factual assessment of the current status of information security in healthcare is vital to the security management of EHR as well. Cybersecurity that contributes to patient safety is part of Saudi Vision 2030, an overarching strategy for the secure digitalization of Saudi society and the business world(Mageit, 2020). The current status of digital security in the Saudi healthcare system, specifically in Saudi hospitals, has been investigated in a nationwide study in 2019(Mishah, Bukhari, AlMutairi, & Mohreq, 2019). (See Fig 1).

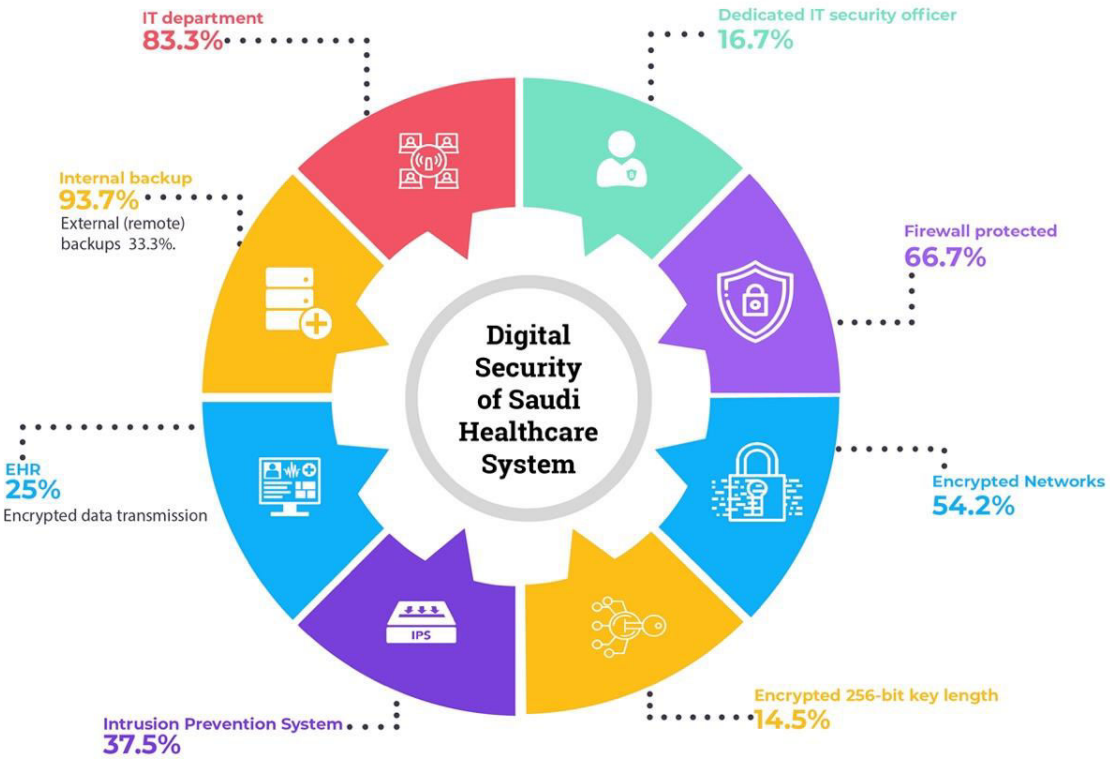

Figure 1 Status of e-Security in Saudi Arabian Hospitals

Based on nearly nationwide data for the Kingdom Saudi Arabia, the authors summarize that IT departments are nearly nationwide in Saudi hospitals. However, this is not the case for health information management departments, which have an organizational/managerial rather than a technical role in managing and protecting health information. According to the Figure 1, most hospitals (83.3%) havesome technical protections in place, such asantivirus software, but often lack policies and organizational protections. For example, only 33.3% of hospitals regularly update their antivirus software, putting the functionality of this protection at risk(Mishah et al., 2019). The authors also suspect a particular bias in the return of the study questionnaire, as some of the IT managers among those interviewed for the study were asked by their supervisors not to share technical details or cybersecurity measures. The researchers conclude that immediate intervention is needed to maintain the privacy and security of patient data in Saudi hospitals as attack vectors are increasing worldwide and in an interconnected computer network, no country can be considered safe from attack(Mishah et al., 2019).

4.6 Usable Security in Healthcare

While the physiological and intellectual prerequisites and needs of users of IT are the same worldwide, some factors relevant to the usability of the computer system differ between countries or regions(Hall, Jong, & Steehouder, 2004). For example, the results of the famous and widely used "Thinking Aloud" method in usability tests differ between citizens from Western (USA, Europe) and Eastern (Asia) countries due to differences in verbal versus nonverbal expression and depend not only on the background of the subjects but also on that of the evaluators(Clemmensen, Hertzum, Hornbæk, Shi, & Yammiyavar, 2009). Other major factors that lead to usability differences between countries are language and writing systems, including signs and symbols more broadly, such as the perceived meaning of and preference for certain colors(Barber & Badre, 1998). These differences must be taken into account when evaluating a system for usability. In the US market in particular, much research has been done on usability issues related to IT systems in healthcare. For example, the US National Institute of Standards and Technology (NIST), the national equivalent of International Standardization Organization (ISO), published guidelines for improving EHR usability back in 2010(Schumacher & Lowry, 2010). Their authors postulate that user-centered design must be implemented in any EHR development process to ensure that the resulting systems are efficient, effective, and satisfying. Interestingly, the document does not address the interdependence of usability and security. The authors simply state that, in general, privacy and security are perceived as primary barriers to the adoption of EHRs in healthcare, but that, according to their research, it is actually a lack of usability that slows the adoption of EHRs(Schumacher & Lowry, 2010). However, other authors have long recognized the complex interactions of security and usability. While there is, or appears to be, a trade-off between security and usability in many contexts, poor usability can also compromise the security of a system, for example, by making it difficult for users to choose appropriate security settings(Kainda et al., 2010). Conversely, poor security also affects usability in the long run, for example, when vulnerabilities are exploited and systems become unavailable and unusable (Audun Jøsang, AlFayyadh, Grandison, Zomai, & McNamara, 2007). In summary, usable security is not sufficiently addressed in the NIST guidelines(Schumacher & Lowry,

2010). Another US group, the Task Force on Usability, located at American Medical Informatics Association (AMIA), has published EHR usability recommendations(Middleton et al., 2013). Although the working group explicitly aims to increase patient safety with its recommendations, information security and usability insecurity are not discussed in the paper. Security and safe use are only considered in the context of patient safety risks, such as alarm fatigue among physicians and nurses that leads to excessive alarm override rates, rendering alarms ineffective, and other potential sources of medical errors caused by poor usability(Middleton et al., 2013). Similar to the NIST guidelines, these recommendations also neglect usability. A Spanish working group has looked more closely at usable security in health records. However, they have focused on the collection and analysis of usability and security in personal health records (PHR) controlled by patients and available on the Internet, and have not analyzed hospital-based EHRs or made their recommendations for the implementation of usable and secure systems(Carrión, Fernández-Alemán, & Toval, 2011; Carrión Señor, Fernández-Alemán, & Toval, 2012).

5 Information Technology Usability in the Arab World

First, usability research is not necessarily transferable between different cultures and regions. Therefore, usability studies with a European or US background may not be relevant to Arabic contexts(Barber & Badre, 1998; Clemmensen et al., 2009; Hall et al., 2004; Schumacher & Lowry, 2010).Furthermore, even though Arabic is one of the world languages with the most significant number of speakers, there is only sparse research on usability issues surrounding Arabic language IT systems(Benabid Najjar, Al-Wabil, Hosny, Alrashed, & Alrubaian, 2021). Second, even if studies with a Western population were unconditionally applicable to Arabic users and systems, there is a lack of evidence-based recommendations regarding usable security in healthcare(Middleton et al., 2013; Schumacher & Lowry, 2010). However, the fact that the issue of usable security in healthcare is culture-dependent and has not been studied comprehensively in any culture is at the same time an opportunity for the Saudi IT and healthcare industries to develop systems that are suited to regional and local conditions in the best possible way. First steps have been made towards genuine Arabic usability research: For example, with mobile applications in mind, a recent paper from the Software Engineering and Computer Science Departments at King Saud and Alfaisal Universities has investigated the optimization of usability of single-pointer keyboards on mobile devices with Arabic keyboard layout(Benabid Najjar et al., 2021). In another study performed by researchers from different Riyadh-based research institutions, Saudi users' preferences regarding Arabic website usability have been investigated. Some of the most noticeable results were users' preference for their native language over English (82%), the importance of websites' (in particular images and graphics) compatibility with Saudi culture and Islamic beliefs (52% and 67%, respectively), and most relevantly to the issues discussed here, the importance of strong security and privacy (78%) and ability to prevent (75%) and to recognize, diagnose and recover (76%) from errors. Based on these results, the authors issued concise cultural usability guidelines for Saudi Arabia(Alyahyan, Aldabbas, & Alnafjan, 2016).

6 Limitation of the study

This study is a narrative review and not a systematic review. This is because there is very little

empirical or other research on the main research question, i.e., the state of usable security and its impact on patient safety and satisfaction in the Saudi healthcare system. Therefore, this study does not present solid and evidence-based recommendations for the development and implementation of usable security in the Saudi healthcare system, but provides insights and directions for further empirical studies.

7 Conclusion

As seen above, there are two crucial facts to consider when considering how to achieve usable safety in Saudi healthcare: first, usability research is not necessarily transferable between different cultures and regions. Therefore, usability studies with a European or US background may not be relevant to Arabic contexts(Barber & Badre, 1998; Clemmensen et al., 2009; Hall et al., 2004). Moreover, although Arabic is one of the world languages with the largest number of speakers, there is sparse research on usability issues around Arabic language-based IT systems(Benabid Najjar et al., 2021). Second, even if studies with a Western population were unconditionally transferable to Arabic users and systems, there is a lack of evidence-based recommendations on usability safety in healthcare(A. Jøsang et al., 2007; Kainda et al., 2010; Middleton et al., 2013; Schumacher & Lowry, 2010). However, the fact that the issue of usable safety in healthcare is culture-dependent and has not been extensively studied in any culture is at the same time an opportunity for Saudi Arabian IT and healthcare. It will help to develop systems that are best suited to regional and local conditions. The current research findings identified in this paper point to gaps in empirical research and suggest future research on usable healthcare security applied to a specific Saudi Arabian background.

Abbreviations

IT = Information Technology
TA = Think Aloud (TA)
HE = Heuristic Evaluation
SSO = Single sign-on
EHRs = Electronic Health Record System
EMR = Electronic Medical Record
HL7 = Health Level 7
FHIR = Fast Healthcare Interoperability Resources
NIST = National Institute of Standards and Technology
ISO = International Standardization Organization
AMIA = American Medical Informatics Association (AMIA)
PHR = Personal Health Records
CIA = Confidentiality, Integrity, and Availability

References

Abd-El-Barr, M. (2021). Evaluation and Performance Comparison of a Model for Adoption of Biometrics in online Banking. *kuwait journal of science, 48*.

Al-Zahrani, F. A. (2020). Evaluating the Usable-Security of Healthcare Software through Unified Technique of Fuzzy Logic, ANP and TOPSIS. *IEEE Access, PP*, 1-1. doi:10.1109/ACCESS.2020.3001996

Alessa, T., S Hawley, M., Alsulamy, N., & de Witte, L. (2021). Using a Commercially Available App for the Self-Management of Hypertension: Acceptance and Usability Study in Saudi Arabia. *JMIR Mhealth Uhealth, 9*(2), e24177. doi:10.2196/24177

AlHogail, A., & Mirza, A. (2014, 17-19 Jan. 2014). *Information security culture: A definition and a literature review.* Paper presented at the 2014 World Congress on Computer Applications and Information Systems (WCCAIS).

Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. *Saudi Medical Journal, 38*(12), 1173-1180. doi:10.15537/smj.2017.12.20631

Alshamrani, M. (2021). IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *Journal of King Saud University - Computer and Information Sciences*. doi:https://doi.org/10.1016/j.jksuci.2021.06.005

Alyahyan, L., Aldabbas, H., & Alnafjan, K. (2016). Preferences of Saudi Users on Arabic Website Usability. *International Journal of Web & Semantic Technology, 7*, 1-8.

Bai, W., Namara, M., Qian, Y., Kelley, P. G., Mazurek, M. L., & Kim, D. (2016). *An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems*. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/bai

Barber, W., & Badre, A. N. (1998). *Culturability: the merging of culture and usability*.

Benabid Najjar, A., Al-Wabil, A., Hosny, M., Alrashed, W., & Alrubaian, A. (2021). Usability Evaluation of Optimized Single-Pointer Arabic Keyboards Using Eye Tracking. *Advances in Human-Computer Interaction, 2021*, 6657155. doi:10.1155/2021/6657155

Bradford, N. K., Caffery, L. J., & Smith, A. C. (2016). Telehealth services in rural and remote Australia: a systematic review of models of care and factors influencing success and sustainability. *Rural & Remote Health, 16*(4), 3808. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/27744708

Carrión, I., Fernández-Alemán, J. L., & Toval, A. (2011, 2011//). *Usable Privacy and Security in Personal Health Records.* Paper presented at the Human-Computer Interaction – INTERACT 2011, Berlin, Heidelberg.

Carrión Señor, I., Fernández-Alemán, J. L., & Toval, A. (2012). Are personal health records safe? A review of free web-accessible personal health record privacy policies. *J Med Internet Res, 14*(4), e114. doi:10.2196/jmir.1904

Clemmensen, T., Hertzum, M., Hornbæk, K., Shi, Q., & Yammiyavar, P. (2009). Cultural cognition in usability evaluation. *Interacting with Computers, 21*(3), 212-220. doi:https://doi.org/10.1016/j.intcom.2009.05.003

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal, 189*(22), E786. doi:10.1503/cmaj.1095434

Cranor, L., & Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems that People Can Use*.

Das, S., Dingman, A., & Camp, L. J. (2018, 2018//). *Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key.* Paper presented at the Financial Cryptography and Data Security, Berlin, Heidelberg.

Dykstra, J. (2020). *Invisible Security: Protecting Users with No Time to Spare*.

Dykstra, J., & Spafford, E. H. (2018). The case for disappearing cyber security. *Communications of the ACM, 61*(7), 40-42.

Everson, J., & Butler, E. (2020). Hospital adoption of multiple health information exchange approaches and information accessibility. *J Am Med Inform Assoc, 27*(4), 577-583. doi:10.1093/jamia/ocaa003

Ganiga, R., Pai , R. M., Pai, M. P., & Sinha, R. K. (2020). Security framework for cloud based Electronic Health Record (EHR) system. *International Journal of Electrical and Computer Engineering, 10*(1), 455-466. doi:https://doi.org/10.11591/ijece.v10i1.pp455-466

Garfinkel, S., & Lipford, H. (2014). *Usable Security: History, Themes, and Challenges.*

Hall, M., Jong, M. D., & Steehouder, M. (2004). Cultural differences and usability evaluation. Individualistic and collectivistic participants compared. *Technical Communication, 51*, 489-503.

Healthcare Cybersecurity-HIPPA Journal. (2021). Retrieved from https://www.hipaajournal.com/category/healthcare-cybersecurity/

Herzberg, A., & Margulies, R. (2013, 23-24 May 2013). *Conducting ethical yet realistic usable security studies.* Paper presented at the 2013 IEEE Security and Privacy Workshops.

Horgan, D., Hackett, J., Westphalen, C. B., Kalra, D., Richer, E., Romao, M., . . . Montserrat, A. (2020). Digitalisation and COVID-19: The Perfect Storm. *Biomedicine Hub, 5*(3), 1-23. doi:10.1159/000511232

Ibarra, J., Jahankhani, H., & Kendzierskyj, S. (2019). *Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime*.

Issa, A., Murray, T., & Ernst, G. (2018). *In search of perfect users: towards understanding the usability of converged multi-level secure user interfaces*. Paper presented at the Proceedings of the 30th Australian Conference on Computer-Human Interaction, Melbourne, Australia. https://doi.org/10.1145/3292147.3292231

James, N., Marwaha, S., Brough, S., & John, T. T. (2020). Impact of Single Sign-on Adoption in an Assessment Triage Unit: A Hospital's Journey to Higher Efficiency. *J Nurs Adm, 50*(3), 159-164. doi:10.1097/NNA.0000000000000860

Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M., & McNamara, J. (2007, 10-14 Dec. 2007). *Security Usability Principles for Vulnerability Analysis and Risk Assessment.* Paper presented at the Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007).

Jøsang, A., AlFayyadh, B., Grandison, T., Zomai, M., & McNamara, J. (2007). *Security Usability Principles for Vulnerability Analysis and Risk Assessment*.

Ka-Ping, Y. (2004). Aligning security and usability. *IEEE Security & Privacy, 2*(5), 48-55.

doi:10.1109/MSP.2004.64

Kainda, R., Fléchais, I., & Roscoe, A. W. (2010, 15-18 Feb. 2010). *Security and Usability: Analysis and Evaluation.* Paper presented at the 2010 International Conference on Availability, Reliability and Security.

Kaplan, B. (2020). REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. *Int J Med Inform, 143*, 104239. doi:10.1016/j.ijmedinf.2020.104239

Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*. doi:https://doi.org/10.1016/j.jksuci.2021.01.018

Kelpsas, B., & Nelson, A. (2016). Ransomware in Hospitals: What Providers Will Inevitably Face When Attacked. *J Med Pract Manage, 32*(1), 67-70.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*. doi:https://doi.org/10.1016/j.eij.2020.07.003

Khajouei, R., & Farahani, F. (2020). A combination of two methods for evaluating the usability of a hospital information system. *BMC Med Inform Decis Mak, 20*(1), 84. doi:10.1186/s12911-020-1083-6

Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2020, 2020//). *Exploring the Meaning of "Usable Security"*. Paper presented at the Human Aspects of Information Security and Assurance, Cham.

Mageit, S. (2020). Saudi Vision 2030: Cybersecurity through the lens of patient safety [Internet]. Retrieved from https://www.healthcareitnews.com/news/emea/saudi-vision-2030-cybersecuritythrough-

lens-patient-safety

Martin, G., Kinross, J., & Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. *BMJ, 357*, j2375. doi:10.1136/bmj.j2375

Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., . . . American Medical Informatics, A. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. *J Am Med Inform Assoc, 20*(e1), e2-8. doi:10.1136/amiajnl-2012-001458

Mishah, N., Bukhari, A., AlMutairi, B., & Mohreq, M. (2019). Status of e-security and privacy protection in Saudi hospitals. *Computer Methods and Programs in Biomedicine, 171*, 5-6. doi:https://doi.org/10.1016/j.cmpb.2018.12.012

Peikari, H. R., T, R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Med Inform Decis Mak, 18*(1), 102. doi:10.1186/s12911-018-0681-z

Powell-Cope, G., Nelson, A. L., & Patterson, E. S. (2008). Patient Care Technology and Safety. In *Patient Safety and Quality: An Evidence-Based Handbook for Nurses.*: Rockville (MD): Agency for Healthcare Research and Quality (US).

Sahu, K., Pandey, R., & Kumar, R. (2014). Risk Management Perspective in SDLC. *International Journal of Computer Science and Software Engineering, 4*, 1247-1251.

Sahu, K., & Pandey, R. S. (2015). Stability: Abstract Roadmap of Software Security. *American International Journal of Research in Science, Technology, Engineering & Mathematics, 2*, 183-186.

Saltzer, J. H., & Schroeder, M. D. (1975). *The protection of information in computer systems.* Paper presented at the Proceedings of the IEEE.

Saripalle, R., Runyan, C., & Russell, M. (2019). Using HL7 FHIR to achieve interoperability in patient health record. *J Biomed Inform, 94*, 103188. doi:10.1016/j.jbi.2019.103188

Schumacher, R., & Lowry, S. (2010). NIST guide to the processes approach for improving the usability of electronic health records. Retrieved from https://www.nist.gov/system/files/documents/itl/hit/Guide_Final_Publication_Version.pdf

Security, R. (2019). WHAT ARE THE DIFFERENT TYPES OF IT SECURITY? *IT Security & Cybersecurity Awareness Training*. Retrieved from https://blog.rsisecurity.com/what-are-the-different-types-of-it-security/

Smetters, D. K., & Grinter, R. E. (2002). *Moving from the design of usable security technologies to the design of useful secure applications*. Paper presented at the Proceedings of the 2002 workshop on New security paradigms, Virginia Beach, Virginia. https://doi.org/10.1145/844102.844117

Sohaib, O., Naderpour, M., Hussain, W., & Martinez, L. (2019). Cloud computing model selection for e-commerce enterprises using a new 2-tuple fuzzy linguistic decision-making method. *Computers & Industrial Engineering, 132*, 47-58. doi:https://doi.org/10.1016/j.cie.2019.04.020

Spence , N., Paul III, D. P., & Coustasse, A. (2017). *Ransomware in Healthcare Facilities: The Future is Now.* Paper presented at the Management Faculty Research Management, Marketing and MIS (Fall 2017).

Storer, T., Marsh, S., Noël, S., Esfandiari, B., El-Khatib, K., Briggs, P., . . . Bicakci, M. V. (2013, 10-12 July 2013). *Encouraging second thoughts: Obstructive user interfaces for raising security awareness.* Paper presented at the 2013 Eleventh Annual Conference on Privacy, Security and Trust.

Theofanos, M. (2020). *Is Usable Security an Oxymoron?* : NIST: National Institute of Standards and Technology Retrieved from https://csrc.nist.gov/CSRC/media/Projects/usable-cybersecurity/images-media/Is%20Usable%20Security%20an%20Oxymoron.pdf

Thimbleby, H. (2013). Technology and the future of healthcare. *Journal of public health research, 2*(3), e28-e28. doi:10.4081/jphr.2013.e28

Vega-Barbas, M., Seoane, F., & Pau, I. (2019). Characterization of User-Centered Security in Telehealth Services. *International Journal of Environmental Research and Public Health, 16*(5), 693. doi:10.3390/ijerph16050693

Whitten, A., & Tygar, J. D. (1999). *Why Johnny can't encrypt: a usability evaluation of PGP 5.0*. Paper presented at the Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, Washington, D.C.

Yeng, P. K., Fauzi, M. A., & Yang, B. (2020, 10-13 Dec. 2020). *Comparative analysis of machine learning methods for analyzing security practice in electronic health records'*

logs. Paper presented at the 2020 IEEE International Conference on Big Data (Big Data).

Zurko, M. E. (2005). *User-centered security: Stepping up to the grand challenge.* Paper presented at the 21st Annual Computer Security Applications Conference (ACSAC'05).

Zurko, M. E., & Simon, R. T. (1996). *User-centered security.* Paper presented at the Proceedings of the 1996 workshop on New security paradigms.