Multi-Factor Authentication for Secured Access Control to Electronic Health Records in South African Public Hospitals

Kabelo Chuma Jr, Mandisa Msomi Jr

Submitted to: Journal of Medical Internet Research
on: July 30, 2024

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on it's website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressively prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

Multi-Factor Authentication for Secured Access Control to Electronic Health Records in South African Public Hospitals

Kabelo Chuma Jr[1*]; Mandisa Msomi Jr[1*] MD

[1]Department of Information Science University of South Africa College of Human Sciences Pretoria ZA
[*]these authors contributed equally

Corresponding Author:
Kabelo Chuma Jr
Department of Information Science
University of South Africa
College of Human Sciences
Preller St
Muckleneuk
Pretoria
ZA

Abstract

Background: In this rapidly advancing digital landscape, the security of Electronic Health Records (EHRs) is increasingly dependent on robust authentication and access control measures. Despite advancements in cybersecurity, South African public hospitals are particularly vulnerable and targeted by cyber-attacks and data breaches due to vulnerabilities associated with username and password-based authentication. These vulnerabilities pose substantial risks to the security and privacy of EHRs and cause huge disruptions to public hospitals.

Objective: With the potential to cause widespread disruption and harm, this study aims to propose a framework for integrating Multi-Factor Authentication (MFA) to enhance to user authentication and access control to EHRs in South African public hospitals.

Methods: A qualitative research design was employed to understand security vulnerabilities and risks in password authentication within public hospitals. The study conducted semi-structured interviews with 15 purposively selected IT technicians, network controllers, and IT managers working in public hospitals. All interviews were audio-recorded, transcribed verbatim, and analyzed using thematic analysis and NVivo version 12. The study applied a conceptual framework grounded in Protection Motivation Theory.

Results: The analysis revealed that public hospitals experienced authentication vulnerabilities such as username enumeration, broken authentication, weak credentials, and credential leakage. Phishing, cryptojacking, ransomware, and password attacks were among the security incidents encountered in public hospitals. Participants expressed that security vulnerabilities in hospitals are due to weak and easily guessable passwords created by staff, the reuse of the same password across multiple systems, irregular password updates, reliance on legacy systems, writing down passwords on paper, and the lack of regular updates to Windows Firewall and Microsoft Defender Antivirus.

Conclusions: The study emphasizes the need for developing robust password policies, modernizing legacy systems, and promoting cybersecurity awareness training in public hospitals. Furthermore, the study suggested a framework for public hospitals to effectively address authentication vulnerabilities. and reinforcing data security. The research underscores that, despite the ongoing vulnerabilities and weaknesses of password and username-based authentication, the study concludes that the integration of MFA offers a scalable solution to significantly improve the security and access control of EHRs in public hospitals.

(JMIR Preprints 30/07/2024:64918)
DOI: https://doi.org/10.2196/preprints.64918

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.

Only make the preprint title and abstract visible.

No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Multi-Factor Authentication for Secured Access Control to Electronic Health Records in South African Public Hospitals

[1]Kabelo Given Chuma
chumakg@unisa.ac.za
ORCID: 0000-0002-5817-6063
Department of Information Science, University of South Africa, Pretoria, South Africa
[2]Mandisa Msomi
msomim@unisa.ac.za
ORCID: 0000-0002-5751-9765
Department of Information Science, University of South Africa, Pretoria, South Africa

Corresponding author's email: chumakg@unisa.ac.za

Abstract

Background: In this rapidly advancing digital landscape, the security of Electronic Health Records (EHRs) is increasingly dependent on robust authentication and access control measures. Despite advancements in cybersecurity, South African public hospitals are particularly vulnerable and targeted by cyber-attacks and data breaches due to vulnerabilities associated with username and password-based authentication. These vulnerabilities pose substantial risks to the security and privacy of EHRs and cause huge disruptions to public hospitals.

Objective: With the potential to cause widespread disruption and harm, this study aims to propose a framework for integrating Multi-Factor Authentication (MFA) to enhance to user authentication and access control to EHRs in South African public hospitals.

Methods: A qualitative research design was employed to understand security vulnerabilities and risks in password authentication within public hospitals. The study conducted semi-structured interviews with 15 purposively selected IT technicians, network controllers, and IT managers working in public hospitals. All interviews were audio-recorded, transcribed verbatim, and analyzed using thematic analysis and NVivo version 12. The study applied a conceptual framework grounded in Protection Motivation Theory.

Results: The analysis revealed that public hospitals experienced authentication vulnerabilities such as username enumeration, broken authentication, weak credentials, and credential leakage. Phishing, cryptojacking, ransomware, and password attacks were among the security incidents encountered in public hospitals. Participants expressed that security vulnerabilities in hospitals are due to weak and easily guessable passwords created by staff, the reuse of the same password across multiple systems, irregular password updates, reliance on legacy systems, writing down passwords on paper, and the lack of regular updates to Windows Firewall and Microsoft Defender Antivirus.

Conclusions: The study emphasizes the need for developing robust password policies, modernizing legacy systems, and promoting cybersecurity awareness training in public hospitals. Furthermore, the study suggested a framework for public hospitals to effectively address authentication vulnerabilities. and reinforcing data security. The research underscores that, despite the ongoing vulnerabilities and weaknesses of password and username-based authentication, the study concludes that the integration of MFA offers a scalable solution to significantly improve the security and access control of EHRs in public hospitals.

Keywords:
Multi-factor authentication, data security, access control, authentication, cyber-attacks, Electronic Health Records, Public hospitals, data breaches.

Introduction and background

User authentication together with access control for Electronic Health Records (EHRs) serve as fundamental pillars of digital security in healthcare environment. They play the most vital role in protecting the most sensitive and confidential personal health information about patients in healthcare facilities. [1,2] advocate that authentication and access control system are critical aspects of healthcare to protect patients' privacy and health information in EHR systems. In today's digital fast paced world, where data theft, cyberattacks, and data breaches are becoming more prevalent and more sophisticated and lucrative, it is essential for healthcare facilities to effectively implement robust authentication and maintain proper digital access controls to protect EHRs against unauthorised access, use, disclosure, and modification. In support of this assertion, [3] advocate the view that healthcare providers and organisations must prioritise the implementation of strong and effective security protocols such as access control systems, authentication, and log analysis to adequately protect EHRs in the cloud against cyber-attacks and breaches.

With the exponential increase in cyber-attacks and data breaches, protecting EHRs has become a significant challenge. This is largely due to the fact that many healthcare providers and hospitals worldwide continue to rely on Single-Factor Authentication (SFA) as their primary security mechanism [4,5]. Similarly, [6] affirm that hospitals, clinics, and healthcare-related organisations. are particularly vulnerable to data breaches because of using outdated, and obsolete systems that uses SFA, and in most cases this is a simple username and password. As a matter of fact, there is no doubt that SFA on publicly accessible systems is perceived as a common source of cyber-attacks and data breaches in the healthcare industry as a whole. [1,7] caution that SFA is particularly more vulnerable to data breaches and cyber-attacks, and it is not a suitable mechanism for systems handling sensitive information.

In line with this conceptualisation, the South African healthcare sector continues to grapple with a myriad of cybersecurity threats ranging from unauthorised access, data breaches, insider threats to password attacks. [8,9] affirm that the healthcare industry in South Africa has become a lucrative target for cyber-criminal activities because of the increasing dependence on EHRs and health systems. Subsequently, Healthcare practices and facilities around the country have become more susceptible to cyber-attacks and data breaches-disrupting systems and services and compromising the integrity, availability, and confidentiality of the EHRs [10]. To support this notion, [11] substantiates that South Africa's leading hospitals and healthcare organisations have been victimised by large-scale cyber-attacks and data breaches since the onset of the COVID-19 pandemic. For instance, a report by [12] revealed that more than 36% of hospitals in South Africa had experienced security incidents ranging from ransomware attacks, and data breaches to phishing attacks, threatening day-to-day IT operations.

As a consequence, the reason behind the frequency and severity of data breaches and cyber threats in South African healthcare is that the vast majority of hospitals still rely on outdated infrastructure, unsupported software, and legacy outdated systems, which use a single factor authentication as a means of securing EHRs. The overwhelming evidence from previous research studies demonstrates that most of the South African public sector health facilities remain plagued by cybersecurity threats due to the increasing dependency on legacy systems that require users to log in using a username and password to access patient information, such as diagnoses, medical history, and medications [10,13,14]. There is no doubt that legacy systems and traditional password authentication do not provide sufficient security for EHRs in cloud computing environments because they were built with outdated technology. [15] attest that outdated legacy systems with password-based authentication pose a range of security risks for healthcare organisations, making them more susceptible to cyberattacks and data breaches.

[16] further stipulate that use of usernames and passwords in hospitals can expose EHRs, health systems and networks to various cyberattacks, including phishing, social engineering attacks, ransomware, and malware. Given this context, Protecting EHRs in South African hospitals remains a complex challenge due to the reliance on usernames and passwords as the primary mechanisms for securing patients' health information. In response to the complex challenges faced by South African public hospitals, there is an urgent need for the integration of Multi-Factor Authentication (MFA) to provide a greater level of data security and protect the confidentiality, integrity, and availability of patient’s health information in the EHR systems from any illegal access. [17] suggest that healthcare facilities and hospitals must adopt third-party MFA to support large-scale healthcare systems and protect their sensitive information against data breaches and unauthorised data access. Nevertheless, MFA emerge as a robust solution to address the challenges facing hospitals, clinics and healthcare-related organisations when safeguarding EHRs [18].

Considering password and username pose serious threat to EHRs security, the South African government, and the Department of Health (DoH) have intensified efforts to improve access control to substantially reduce the risk of security threats to EHRs. These efforts include the implementation of access control policies and programs, conducting internal audits, and training and educating staff. Despite the earnest efforts of the government and DoH, improving access control for EHRs remains an ongoing challenge and concern for most public hospitals in South Africa. Therefore, this study seeks to tackle the urgent need for improving user authentication and access control in South African public hospitals. The findings of this study can be used to improve user authentication and access control for EHRs in the hospitals.

Problem statement

Data security is one of the most pressing challenges facing many healthcare organisations of all sizes. [19] advocate the view that weak authentication protocols and inadequate access controls remain among the leading causes of cyber-attacks and security breaches in digital healthcare. Several scholars have demonstrated that the South African healthcare industry is plagued by a myriad of cyber-attacks and data breaches, which threaten the integrity of patient information and EHR systems [20,21,22]. Consequently, these cyber-attacks are exacerbated by numerous factors, including the widespread use of obsolete legacy systems, obsolete and weak infrastructure, data silos and overreliance on passwords and usernames [23,24,25]. The problem at hand may be articulated as the fact that South African public hospitals continue to use traditional username-password authentication for EHR systems, which contain highly sensitive health information, including patients' identities, medications, diagnoses, medical conditions, and medical histories.

Because of the overreliance on username and password authentication for EHRs, South African public hospitals remain persistently vulnerable to malicious actors, password cracking, and various other cyber-attacks. [26] attest that weak and default passwords and human errors are among the culprit behind data breaches and cyber-attacks facing South African public hospitals. Furthermore, [27,28] emphasize that many hospitals and healthcare organisations in South Africa remain at risk due to their reliance on usernames and passwords that are weak, shared, or reused for accessing EHRs. This leaves them vulnerable to cyber threats such as password cracking and malicious attacks, perpetually compromising their security and privacy [26]. According to the Verizon Data Breach Investigations Report, over 78% of data breaches in South African healthcare are due to broken authentication, compromised or stolen access credentials, human errors, and poorly configured firewalls [29]. Nevertheless, these emerging cyber-attacks coupled with data breaches undermine the overall security posture of South African public sector hospitals, resulting in significant financial and reputational damage.

In response to the situation, the South African National Department of Health has implemented several initiatives to enhance the security of password and username authentication and mitigate the risks of cyber-attacks against EHR systems [30]. For instance, some of the notable efforts by DoH include continuous monitoring and auditing of compliance with authentication protocols, provision of National Cyber Security Centre guidelines, and investment in cybersecurity research [30]. Despite the efforts by DoH, improving the security of password and username authentication remains a complex challenge due numerous factors such as legacy systems, resource constraints, and compatibility issues. Given this situation, addressing the sophistication of cyber-attacks and data breaches threatening South African public hospitals requires a multifaceted approach that includes continuous investment in MFA to improve user authentication for EHRs. [31,32] emphasise that MFA has emerged as a fundamental solution to enhance security and minimize cyber risks due to human error and password misplacement as well as strengthening the overall security posture of healthcare organisations.

As a consequence, there is an apparent need for South African public hospitals to embrace the MFA to fortify data security and protect the sensitive and confidential in-formation held in systems and databases. [33] stress that security frameworks and models are necessary to assist hospitals, and healthcare-related organisations in thwarting, detecting, and/or minimising vulnerabilities, cyber-attacks, and threats against their electronic healthcare systems. In South Africa, several studies have been conducted on cybersecurity in healthcare [9], the security of EHRs [34], and the security and privacy of health data [35]. However, none of these studies have focused on understanding the user authentication vulnerabilities related to the use of usernames and passwords and the effectiveness of MFA in mitigating cyber-attacks. Therefore, this study aimed to address this gap by proposing a framework for integrating MFA to en-hance user authentication and access control for EHRs in South African public hospitals, ultimately reducing the risks of cyber-attacks and data breaches. In order to achieve the stated objective, the following research objectives were explored:

- To establish authentication mechanisms for EHRs in South Africa public hospitals.
- To determine authentication vulnerabilities in EHRs in South African public hospitals.
- To examine security authentication risks to EHRs in South Africa public hospitals.
- To propose a framework for integrating MFA to improve access control for EHRs in by South African public hospitals.

Conceptual framework

A conceptual framework is one of the most foundational components of any re-search study, serving as the basis for the study, guiding the process of research and providing a framework for analysis. [36] defines a conceptual framework as a “network of interrelated concepts or constructs that together provide a comprehensive under-standing of a phenomenon or phenomena under investigation”. The purpose of a conceptual framework is to facilitate the interpretation of research findings and the ability to make connections between empirical findings and existing theories or knowledge in the field [37].

Overall, it serves as a road map to guide the entire research endeavour, from the formulation of the hypothesis to the analysis and interpretation of the results [38]. The researchers developed a conceptual framework informed by the literature review and Protection Motivation Theory (PMT) to guide the study and understand the phenomenon. Figure 1. Illustrates the conceptual framework for the study.

Figure 1: Conceptual Framework

As depicted in Figure 1, the study used a critical concept identified during the literature review to construct a conceptual framework. The construct includes EHRs. The conceptual framework underscores the crucial need to prioritize data security in EHRs through the implementation of robust authentication and rigorous access controls. On the other hand, the researcher also found critical constructs from the PMT to develop the conceptual framework. According to [39,40] stress that PMT is acknowledged as instrument in understanding and explaining cybersecurity behaviours in organisational and institutional context. In particular, this theory can be applied to understand the behaviour of individuals, organisations, and institutions such as healthcare facilities in response to cyber-attacks and data breaches, and to better predict how they will respond to such attacks [41]. [40] stresses that PMT can be applied to identify the cognitive processes that lead to threat perception and the motivation to take protective measures.

According to [42,43], the PMT offers a framework to grasp and encourage cybersecurity behaviours by considering individuals' perceptions of risk, vulnerability, self-efficacy, and response efficacy. Given the above discussion, the researchers used constructs from this theory towards the development of the conceptual framework. The constructs include (a) risk, (b) vulnerability, and (c) response-efficacy. On the other hand, self-efficacy expectancy was not applied in this study. Consequently, the conceptual framework offered a valuable theoretical perspective for understanding security risks and vulnerabilities to EHRs and enhancing the response efficacy of authentication mechanisms such as the MFA by demonstrating its effectiveness in improving authentication and access control in South African public hospitals as well as preventing cyber-attacks and data breaches to EHRs.

Literature review

The literature review for this study was informed by themes emerged from research objectives, including authentication mechanisms for EHRs in healthcare, authentication vulnerabilities in healthcare, and security authentication risks to EHRs in healthcare.

Authentication mechanisms for EHRs in healthcare

Authentication is considered the most important security method for protecting sensitive data, computer systems, and networks from unauthorised attacks [44,45]. There are various authentical mechanisms that are used to protect EHRs against unauthorised access. According to [16], usernames and passwords, also known as the Secure File Access method, are among the most commonly used techniques by healthcare facilities to protect the privacy and security of patient information. He further states that usernames and passwords are inherently prone to a variety of security risks, leaving healthcare facilities and hospitals vulnerable to attacks and breaches [16]. In particular, biometric authentication has become a more common method for securing EHRs in hospitals, clinics, and other healthcare setting.

[46] argue that healthcare facilities have been at the forefront of biometric access control system adoption, particularly for securing access to sensitive healthcare records and facilitating access to systems. This technology has the potential to eliminate fraud or identity theft in the healthcare environment [47]. The literature review demonstrated that authentication protocols such as smartcard, fingerprint or facial recognition, speech patterns, and digital signature are critical in healthcare to protect patients EHRs against unauthorized access or misuse of EHR data [48,49,50].

Authentication vulnerabilities in EHRs in healthcare

EHRs are vulnerable to authentication issues, which can potentially compromise patient data security [51]. There is no doubt that weak or inadequate authentication mechanisms and misconfigured access controls pose significant vulnerabilities in EHRs. [52] that security vulnerabilities can compromise health system operations and jeopardize the accessibility, confidentiality, integrity, and availability of EHRs in the healthcare sector. There is no doubt that hospitals and healthcare-related organisations face authentication vulnerabilities from various threat actors. For instance, [53] state that a host of security vulnerabilities, including the DoS, unauthorised access, ARP poisoning, VM backdoors, hypervisor attacks, rootkit attacks, and VM escape, pose the highest risks to the privacy and security of patient information in healthcare landscape. In contrast, username enumeration, weak passwords, session hijacking, broken authentication, and credential stuffing, weak login credentials are among the most common vulnerabilities related to authentication in healthcare [54,55,56].

Cybercriminals and attackers exploit these vulnerabilities to gain unauthorised access and exploit EHRs [57]. Research studies have found that healthcare facilities worldwide are encountering multiple authentication vulnerabilities due to the growing digitization of their systems. These vulnerabilities include brute-force attacks, password stuffing, HTTP Basic Authentication, and SQL injections, all stemming from inadequate authentication mechanisms [58,59,60]. These authentication vulnerabilities provide cyber criminals and hackers with the opportunity to access health systems and steal sensitive patients' health information for financial and political gains. According to [61], the current certification methods for EHR systems may fail to identify common vulnerabilities at the code and design levels. This might result in the exposure of user login information and unauthorised access to sensitive patient data [62]. In order to tackle these problems, researchers have put up a range of authentication approaches. [63] devised a technique that employs elliptic curve encryption and lightweight hash functions to bolster both security and speed.

In their work, [64] proposed a method that ensures privacy by combining role-based access control with multi-factor authentication. Nevertheless, biometric-based authentication techniques may exhibit vulnerabilities, including recognition failures and susceptibility to insider attacks [65]. These studies emphasise the continuous difficulties in ensuring the security and privacy of EHRs and stress the need to use strong and diverse authentication methods to safeguard sensitive patient data in healthcare systems.

Security authentication risks to EHRs in healthcare

The sensitive nature of patient data is a significant concern, and security authen-tication hazards to EHRs in healthcare are a significant concern. Weak authentication mechanisms and flawed access control pose a significant threat to the security of EHRs in the healthcare domain [66]. There is no doubt that many hospitals, clinics, and healthcare organisations are susceptible to cybersecurity threats and attacks due to weaknesses or gaps in authentication, such as weak login credentials. [67] underscore that malicious actors exploit vulnerabilities from weak authentication and access control to launch numerous cyberattacks such as phishing, social engineering, ransomware, malware and spoofing to access computer systems for stealing health information in hospitals. [26,68,69] advocate that healthcare organisations and hospitals have been victims of ransomware phishing, spam emails, data breaches, viruses, and malware that pose a threat to patients and EHRs because of the use of weak or insecure passwords and username, delayed security updates and other poor security practices.

These cybersecurity threats and attacks have the potential to paralyse the digital infrastructure in healthcare practices, disrupt healthcare systems, and cause serious damage to EHRs [67,68]. Effective implementation of security measures requires col-laboration among healthcare providers, IT specialists, and regulatory bodies to ensure the confidentiality and integrity of sensitive health information [70].

Materials and methods

This study was conducted in the public hospitals located in the Northwest Province in South Africa. The names of hospitals remained anonymous because of the sensitive nature of the study. The study employed a qualitative research method to delve deep into participant’s perceptions and experiences relating to authentication and access control for EHRs in public hospitals. This method allowed participants' voices to be heard and offered inclusive perspectives and insights. Semi-structured interviews were conducted with 15 selected IT technicians, net-work controllers, and IT managers, all of whom had relevant experiences and insights about authentication and access control in public hospitals. These professionals provided valuable perspectives on the daily challenges and security vulnerabilities they encounter with password authentication. The interviews provided a balanced approach by maintaining consistency across all respondents, while also allowing flexibility to explore newly emerging issues in-depth [71]. All participants were approached through e-mails and face-to-face interactions at hospitals, in their respective offices.

Confidentiality of the participants was maintained throughout the entire process as interviews were conducted in private rooms. Semi-structured interviews were con ducted between September 2022 and January 2023. Interviews were audio recorded in hospitals after obtaining permission from the participants. Interview sessions took about 15-20 minutes. The researchers, with the participants' permission, took field notes during the interviews. The researchers first transcribed each audio recording verbatim, listened to the recordings several times, and then went over the transcriptions to gain a deeper understanding of each audio recording. Prior to starting the interviews, all participants were required to sign an informed consent form. Participants' voluntary involvement was emphasised, and they were in-formed of their prerogative to withdraw from the study without any consequences. The transcripts of the interviews were returned to participants for verification or feedback. Moreover, data were analysed using NVivo version 12.

Transcripts were analyzed using a thematic analysis after the data collection process was complete. Approval to conduct this study was granted by the Provincial Health Research Committees. Confidentiality and privacy were maintained during data collection by not using real identifiers. Participants were assigned unique codes or pseudonyms corresponding to the order of the interviews. Additionally, names of hospitals were removed from transcripts to ensure they were de-identified during the transcription of the interviews.

Results

This section presents the findings of this study. The results of 15 participants' interviews were studied and analysed. The study comprised nine male participants and six female participants working in selected public hospitals. Their working experience ranged from 2 to 35 years. Seven of them had a National Diploma in Information Technology (IT), six of them had a Bachelor of Technology (BTech) in IT and Computer Science, while two of the participants had certificates in IT. Table 1. Presents demo-graphic information of the participants.

Table 1: Demographic information of the participants

Code	Position	Qualification	Gender	Experience	Hospital
PH1	IT Technician	Diploma	Male	8	Hospital A
PH2	IT Technician	Diploma	Female	2	Hospital A
PH3	Network Controller	Diploma	Male	11	Hospital C
PH4	Senior IT Manager	BTech	Female	35	Hospital B
PH5	IT Technician	Diploma	Female	4	Hospital D
PH6	Network Controller	Diploma	Male	7	Hospital B
PH7	Network Controller	BTech	Male	10	Hospital A
PH8	IT Technician	IT Certificate	Male	4	Hospital D
PH9	IT Manager	BTech	Female	19	Hospital C
PH10	IT Technician	BTech	Male	5	Hospital B
PH11	Network Controller	Diploma	Female	9	Hospital A
PH12	IT Technician	IT Certificate	Male	2	Hospital D
PH13	Senior IT Manager	BTech	Male	25	Hospital B
PH14	IT Technician	Diploma	Female	8	Hospital A
PH15	IT Manager	BTech	Male	28	Hospital D

(Source: Field data 2022-2023)

Authentication mechanisms for EHRs in public hospitals

Authentication mechanisms are essential in EHRs to protect the privacy and confidentiality of health information of the patient [72,73]. The conceptual framework proposed in conjunction with the literature review has served as an anchor for understanding authentication mechanisms that are used for EHRs. Participants were asked to share their knowledge and experience about authentication mechanisms used in public hospitals to authenticate users to access EHRs. During interviews, most participants expressed that their hospitals use username and password authentication to regulate access to systems and sensitive EHRs. For instance, the participant **(PH3)** said:

"There is no doubt that protecting patient data is of the utmost importance, especially when it comes to electronic health record (EHR) systems. Having said that, in our hospital, we use username-password as the primary authentication method to protect patient data in EHR systems and prevent unauthorized access, data breaches, and identity theft from occurring. In most cases, our employees, doctors, and nurses are required to use their login credentials to be able to access data in the EHR systems".

Another participant **(PH7)** during the interviews offered a similar response. For instance, she said:

"Our hospital uses EHRs that require the users to log in using a login ID and password assigned by our IT division. Doctors, nurses, and other employees are required to log in to the EHR system using their usernames and passwords in order to access and open clinical data related to patients or their health. This is the only mechanism we use for protecting our systems and protecting patient information from breaches, insiders, and disclosure".

Furthermore, participant (PH13) expressed that:

"The authentication mechanism we use in most hospitals in our region is password authentication. We have been using this method for many decades and we have raised numerous concerns and complaints to the Department of Health and the government, highlighting that this mechanism poses serious security challenges and risks to electronic personal health information. We have been urging the government to implement new and reliable secure authentication mechanisms that can permanently replace passwords for authenticating our staff's access to EHRs and Health Information Systems".

As a follow-up question, participants were asked whether they had a password sharing policy in place to prohibit clinical staff and employees from sharing usernames and passwords that provide access to EHR systems and patient data. During the interviews, most of the participants expressed their hospitals had not put in place any password policy that prohibits employees from sharing their passwords with anyone. For instance, the participant **(PH14)** echoes that:

"In our hospital, we do not have password security and sharing policies in place that prohibit employees from sharing their login credentials. This creates a serious problem in our hospitals because most of our colleagues are sharing their login credentials via email, WhatsApp, and other platforms. This is the reason why our sensitive information, systems, and accounts are prone to data breaches and attacks".

On the other hand, participants **(PH1)** and **(PH14)** in the interviews expressed that:

"Our hospital has not implemented any formal password-sharing policy that prevents staff from sharing their login credentials with others. Having said that, most of the colleagues are sharing their credentials amongst each other and the downside of this is the fact that this gives rise to security vulnerabilities and issues in our hospital.

"No, we do not have any written password-sharing policy in place that regulate the sharing of password and username".

Authentication vulnerabilities in public hospitals

The proposed conceptual framework demonstrated a clear understanding of the authentication vulnerabilities. Authentication vulnerabilities of EHRs remains a significant threat to the sanctity of the global healthcare industry. [74,75] advocate that hacktivists, cybercriminals, and attackers exploit vulnerabilities using various tactics to gain unauthorised access to computer systems and networks to commit fraudulent activities. Participants were asked to share their experiences about vulnerabilities they had encountered in their hospitals. During the interviews, participants mentioned password sharing, weak credentials, misconfigurations, credential stuffing, unsecured Wi-Fi access, broken authentication as well as username enumeration as vulnerabilities encountered in their hospitals. For example, one of the participants **(PH13)** said:

"The most common vulnerabilities that we regularly encounter in our hospital are weak passwords, misconfigurations, credential stuffing, and password sharing. Having these vulnerabilities creates major problems in our hospital and often leads to cyber-attacks and threats that cause system and server crashes most of the time".

In contrast, another participant **(PH4)** expressed that:

"Most of our hospitals in this region experience several security vulnerabilities ranging from weak or insecure passwords, credential stuffing, to broken authentication. We have come to realise that these vulnerabilities in password-based login give hackers the opportunity to launch cyber-attacks to target and damage our computer systems".

Furthermore, participant **(PH3)** alluded that:

"We have been experiencing a number of security vulnerabilities in our hospital especially since the emergence of COVID -19 in South Africa, including username enumeration, weak account/passwords, and failed authentication, as well as unsecured Wi-Fi access points coming from outside of the hospital. As a result of these vulnerabilities, patient data in our EHR systems are at risk of being compromised, losing their integrity, and confidentiality, and being accessible to hackers and cybercriminals".

As a follow-up question, participants were asked to indicate the root causes of authentication vulnerabilities experienced in their hospitals. For instance, participant **(PH15)** expressed that:

"During my years of working in hospitals, I have come to realise that one of the most common reasons for security vulnerabilities in our hospitals can be attributed to weak and stolen credentials and password sharing. There is a tendency among our colleagues to create easily guessable passwords, which are more likely to be exploited by cybercriminals, and the majority of the time, our staff members share their passwords to access EHR systems and patient records. Additionally, one of the main reasons why there are vulnerabilities in our hospitals is that most of our colleagues do not regularly update their passwords, which is one of the main causes of vulnerabilities. In many cases, I have noticed that some employees are using the same password for more than a month, and this leads to many security loopholes in our system. In addition to this, the use of legacy systems in our hospitals also contributes to security vulnerabilities".

Another participant **(PH5)** offered a similar response:

In my opinion, most of the security vulnerabilities in our hospitals are exacerbated by weak passwords. Most of our staff create easily guessable passwords and reuse them across multiple systems. Additionally, some staff members engage in poor security practices, such as writing down their passwords and usernames on pieces of paper. Beyond password and username issues, another significant problem is that Windows Firewall and Microsoft Defender Antivirus are not updated regularly, leaving our systems susceptible to attacks due to unpatched vulnerabilities.

Security authentication risks to EHRs in public hospitals

The conceptual framework proposed provided a scientifically sound basis for understanding security authentication risk associated with EHRs. According to [76], many hospitals and healthcare organisations across the globe are increasingly under threat from cyber-attacks and threats due to a lack of adequate security measures to control access and safeguard patient data and EHRs. The participants were asked to share information on the security authentication risks they had encountered in their hospitals due to the use of passwords and usernames for authentication. During the interviews, participants reported that they had experienced phishing attacks, SQL injection, ransomware, spoofing, cryptojacking, malware attacks, password attacks, and distributed denial-of-service (DDoS) in their hospitals. For example, participant **(PH9)** emphasises that:

"As a matter of fact, one of the most widely experienced cybersecurity attacks in our hospital is the

cryptojacking, DDoS attacks, SQL injection, and malware attacks. These security threats pose the highest risk to our patient privacy and information and compromise the integrity of our EHR systems… In addition to this, we usually experience data breaches and operational disruptions because of these cyber-attacks.

Another participant **(PH2)** said:

"Most of our public hospitals are increasingly susceptible to many security incidents, including ransomware, malware attacks, DDoS attacks, and cryptojacking due to the use of weak credentials in our systems. Nevertheless, the majority of the security incidents are frequently experienced due to compromised credentials and inadequate security measures. Because of these attacks our hospital experiences serious risks such as unauthorised access to patient sensitive information and operational disruptions and clinical delays".

In contrast, participant **(PH7)** expressed that:

"Our hospital continues to grapple with a myriad of cyber-attacks ranging from…spams, phishing emails, to password attacks especially since the onset of the COVID-19 pandemic in our country… Most of our staff members have raised their concern that weak and default passwords coupled with outdated legacy systems are among the top causes of cyber-attacks in the hospital. However, we are trying our level best to put in place security measures to detect, identify, and prevent these emerging attacks".

Discussion of the findings

This section discusses the findings of this study. Based on the findings of this study, it is evident that public hospitals were using a default username and password as an authentication mechanism to control access to EHR systems and sensitive data about patients. The results are in accordance with [77,78] who mentioned that many hospitals and other healthcare facilities use a username or identity (ID) with an associated password as an authentication mechanism to control access to health information sys-tems.

According to [79], passwords and usernames are deemed to be the most common security problem in healthcare. The finding of the study further revealed that public hospitals had not put in place any formal password sharing policy that prohibits passwords and account sharing among employees. The study by [80] also discovered that weak password guessing and hacking have compromised the widely used user ID and password mechanisms for securing access to EMRs, increasing cases of medical identity theft, cyber terrorism, and information system attacks, leading to false financial claims and debts.

Based on this, it is evident that employees are sharing passwords due to the lack of a policy explicitly prohibiting this practice. A study by [81] found that cybersecurity policies and procedures in public hospitals in Ecuador need to be improved to effec-tively respond to emerging threats. A similar study by [82] revealed that staff members share their password with one another to access EHRs in hospitals in Indonesia. Fur-thermore, this finding is similar to a related study by [83] who found that hospital workers were sharing usernames and passwords as they had not yet been able to access the systems and programs, they needed to perform their tasks. On the other hand, [84] substantiate that many healthcare facilities and hospitals face a significant security issue related to the sharing of passwords because due to a lack of password sharing policies that prohibit staff members from sharing passwords.

The results showed that username enumeration, weak credentials, misconfiguration, credential stuffing, poorly configured firewalls and anti-virus, broken authentication, and insecure Wi-Fi access points were among the vulnerabilities encountered in public hospitals. Recent research point to serious cybersecurity flaws in healthcare environment. A similar study by [26] found that threats like worms, Trojan horses, and shortcut viruses compounded by technical vulnerabilities weak authentication and access controls, are faced by South African public hospitals. Participants during the interviews frequently mentioned that security vulnerabilities in public hospitals are often attributed to weak and easily guessable passwords created by staff, the reuse of the same password across multiple systems, irregular password updates, reliance on legacy systems, writing down passwords on paper, and the lack of regular updates to Windows Firewall and Microsoft Defender Antivirus.

This finding aligns with the results of a study by [85], which reported that hospitals and clinical practices in Unite Kingdom use traditional passwords and usernames and legacy systems with absence of security updates, leading to numerous security vul-nerabilities and loopholes. Moreover, it was revealed also that spams, phishing attacks, SQL injection, ransomware, spoofing, cryptojacking, malware attacks, password attacks, and DDoS attacks were among the security incidents experienced in public hospitals.

A similar study was conducted by [69] reported that more than 45% of state hos-pitals and other healthcare organisations had experienced email phishing, ransomware, and spoofing attacks compounded by password loopholes, system weaknesses, and misconfigurations throughout the network. This is identical to the findings in our study. Furthermore, participants from this study expressed that their hospitals had been sub-jected to serious risks that include compromised data integrity, operational disruptions, clinical delays, as well as unauthorised access to sensitive information and data breaches.

Recommendations

Based on the findings, this study makes the following recommendations:

- It is clear from the findings that public hospitals depend on password and username to control access to EHRs and protect the integrity of patient information. While passwords and usernames are not equally reliable and safe, the study recommends the need for public hospitals to implement MFA to strengthen the overall security posture. This mechanism can potentially improve the security of authentication and access control by providing additional layers of verification in public hospitals.
- The finding of the study revealed that public hospitals had not put in place any formal password sharing policy that prohibits password and account sharing among and between employees. Therefore, public hospitals are encouraged to implement and enforce a password sharing policy that prohibits staff from sharing usernames and passwords with other personnel. Furthermore, policymakers, and legislators are encouraged to develop appropriate access control policies that enforce MFA.
- The findings revealed username enumeration, weak credentials, misconfiguration, credential stuffing, poorly configured firewalls and anti-virus, broken authentication, and insecure Wi-Fi access points as the most prevalent security vulnerabilities encountered in hospitals due to weak and easy password created by staff, multiple use of the same password, irregular updating of password, legacy systems, writing down password use papers, and lack of updating windows firewall and Microsoft Defender Antivirus regularly. This study recommends the need for public hospitals to modernize outdated legacy systems or replace them entirely. Public hospitals are urged to conduct periodic vulnerability assessments, regular audits, and penetration testing to proactively identify and address any weaknesses and vulnerabilities in their IT security infrastructure.
- It is recommended that public hospitals regularly update Windows Firewall and Microsoft Defender Antivirus. Additionally, public hospitals should advise staff against writing down and storing passwords in any office. Staff should also be encouraged to use unique and complex passwords to minimize security risks.
- To adequately protect EHRs against phishing attacks, SQL injection, ransomware, data breaches, spoofing, cryptojacking, malware attacks, password attacks, and DDoS attacks, public hospitals must conduct regular cybersecurity awareness training sessions to

educate staff about cybersecurity practices, including password hygiene, recognizing phishing attempts, and reporting suspicious activities.

Proposed framework for integrating MFA

This section presents the MFA framework for integrating MFA for secured access control of EHRs in South African Public Hospitals. The proposed framework is intended to add an extra layer of security, requiring hospital staff to provide multiple forms of identification before accessing EHRs. Nonetheless, the proposed framework aims to enhance the security of EHRs by addressing the identified vulnerabilities and reinforcing data protection measures. Figure 2 depicts the proposed framework.

Figure 2: Framework for integrating MFA

As shown in Figure 2, the motive behind this framework is to improve access control in public hospitals by using a multi-factor authentication for accessing electronic health records. The framework comprises four different layers, including user application, authentication, cloud storage, and regulatory compliance layer. Each is explained as follows.

User access

User access is the authorisation that allows users in the hospital to access systems and information, or data captured in EHRs for patient registries. In this layer, users include doctors, nurses, physicians, clerical personnel, and administrators who are responsible for using EHRs to perform their daily routine clinical and administrative activities in hospitals. Access to EHRs is limited to authorised users. This means that all the users must be authorised to gain access to patient's electronic patient records. In the proposed framework, users are required to go through the login process that can be done on a designated computer workstation. They are required to register with the cloud and create an account with a username and a strong and secured password in line with password policies. Once registration is successful, users should login using the same username and password.

Authentication

Authentication refers to the security process through which hospital users must prove their identities before they are permitted access. Upon entering the username and password, the server will authenticate the users and provide further authentication, which will involve the use of a One-Time Password (OTP) in order to carry out the verification once the login details have been entered. The system will then generate the OTP for the users via e-mail or mobile phone once the login authentication has been verified as successful. The users will be required to login using the OTP provided by the system. As soon as the OTP is provided and verified, the server will authenticate and provide the final biometric authentication, which involves the use of an optical or ultrasonic fingerprint scanner. The authentication system will record and store the pre-captured biometrics before verifying the users. Once the fingerprint verification is completed, the authorised users will be granted access to cloud storage in order to securely access the electronic health records.

Cloud storage

Cloud storage is online storage where EHR data is stored on remote servers and managed and maintained by a third-party provider. In this layer, only authorised users have access to classified information. Nonetheless, the cloud storage in the proposed framework provides three services. The first service includes a centralised database for storing all EHRs. The second service is a file server which acts as remote storage for allowing multiple users on the same network to store and access necessary EHR files. The third service is the audit log. The audit log in this layer is responsible for tracking all admin activities and the actions a user has performed on a system. The purpose of these logs is to assist in identifying how, when, where, why, and by whom data was accessed, modified, and/or leaked in order to identify abuses. Consequently, this forms a part of the system auditing process. It is essential that audit logs be tamper-proof, immutable, and act as a tool to ensure data integrity by ensuring that they provide a consistent audit trail that can enable the discovery of data breaches, as well as the identification of compromised accounts, to be conducted [86]. Once the audit log is performed, the cloud responds with EHR data to access requests from hospital users and transfer them to the hospital EHR server. The hospital EHR server will allow users to access and retrieve data remotely via internet. This server must be protected by dedicated and updated firewalls to prevent reasonably anticipated threats to the security or integrity of the EHRs.

Regulatory compliance

Regulatory compliance is the process of ensuring adherence to laws, guidelines and regulations enacted by the state, federal, or international governments that might apply to a particular organisation or company. Regulatory compliance is a very important aspect of authentication and access control. Public hospitals along with policymakers and legislators must implement and enforce access control policy, password sharing policy, and Standard Operating Procedures (SOPs) that govern how access to EHRs is granted and how systems can be protected against data breaches and cyber-attacks. Moreover, hospital leaders must encourage staff to familiarise themselves with applicable policies, procedures, and requirements for access control.

Conclusions and future work

Cyber-attacks targeting public hospitals that uses EHRs with single authentication such as password and username remain pervasive due to their inherent vulnerabilities. The findings indicate that South African public hospitals were susceptible to phishing attacks, SQL injection, ransomware, spoofing, cryptojacking, malware attacks, password attacks, and DDoS attacks. It was established that public hospitals had suffered from significant security risks, including compromised data integrity, operational disruptions, clinical delays, unauthorized access to sensitive information, and data breaches. Moreover, it is evident that the use of usernames and passwords in public hospitals were compromised due to staff members sharing passwords among themselves. Recognising that usernames and passwords represent one of the weakest security points in South African public hospitals, the researchers proposed a framework for integrating MFA. This framework provides an additional layer of security beyond traditional logins, thereby enhancing the protection of access to EHRs.

The framework in-corporates OTP and fingerprint verification alongside usernames and passwords to create a flexible, efficient, and reliable interface for accessing EHRs. Public hospitals are encouraged to incorporate some of the suggested solution in the framework to improve their authentication and access control for EHRs. This study makes substantial contribution to policy, practice, and theory. In terms of policy, this study provides evidence-based recommendations for policymakers and legislators to strengthen authentication and access control of EHRs, emphasising the integration of MFA as a standard practice in public hospitals. By highlighting the specific vulnerabilities and the effectiveness of MFA, the study leads to the development of more stringent security policies and regulations that mandate the use of advanced authentication technologies. In terms of practice, the study contributes to practice by highlighting the importance of cyber-security awareness training program to educate staff about cybersecurity practices. This proposed framework serves as a guideline for public hospitals to streamline their access control processes, reducing operational disruptions associated with cyber-attacks and data breaches. The combination of empirical data and professional insights ensures proposed solutions are not only theoretically sound but also practically applicable, ultimately aiming to improve authentication and access control in South African public hospitals.

Furthermore, the study advances theoretical understanding through exploring the effectiveness MFA in mitigating cyber-attacks and addressing vulnerabilities and risks associated with traditional authentication methods. This study sets a precedent for future research in the field of healthcare cybersecurity. Ultimately, the study contributes to the broader field of healthcare cybersecurity research, offering a basis for future studies and development in enhancing organisational resilience against evolving cybersecurity attacks and data breaches. For future work, the next step is to have the proposed framework reviewed, tested, and validated by healthcare experts. Once vali-dated, a survey will be distributed to practitioners and expert in the field of healthcare system to confirm the framework, which will then be used as a case study in a re-al-world setting. Another research avenue is to compare the proposed framework against existing MFA frameworks in other developed and developing countries. Furthermore, Future studies can build on this research to explore how MFA can be implemented in South African public hospitals.

Author Contributions: KG Chuma and M Msomi contributed to the conception and design of the study, writing of the paper, critical review of the paper and final approval. All authors provided critical feedback and approved the final version of the manuscript.
Funding: This research received no external funding
Ethical approval: Approval to conduct this study with refence number: NP_202206_076 was granted by the Provincial Health Research Committees
Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.
Data Availability Statement: The data analysed in this study are not publicly available due to privacy and ethical restrictions. Therefore, data can be published upon request.
Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

EHR	Electronic Health Records
DoH	Department of Health
MFA	Multi-Factor Authentication
SFA	Single-Factor Authentication
COVID-19	Coronavirus disease of 2019
PMT	Protection Motivation Theory
SQL	Structured Query Language
HIS	Health Information Systems

Reference

1. Jayabalan, M & O'Daniel, T. 2017. Continuous and transparent access control framework for electronic health records: A preliminary study. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 165-170). IEEE. [doi: 10.1109/ICITISEE.2017.8285487].
2. Liu, Y., Zhang, Y., Ling, J & Liu, Z. 2018. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Generation Computer Systems, 78, pp.1020-1026. [doi: 10.1016/j.future.2016.12.027]
3. Seol, K., Kim, Y.G., Lee, E., Seo, Y.D. and Baik, D.K., 2018. Privacy-preserving attribute-based access control model for XML-based electronic health record system. IEEE Access, 6, pp.9114-9128. [Doi: 10.1109/ACCESS.2018.2800288].
4. Gabriel, M.H., Noblin, A., Rutherford, A., Walden, A. and Cortelyou-Ward, K., 2018. Data breach locations, types, and associated characteristics among US hospitals. Am J Manag Care, 24(2), pp.78-84. [PMID: 29461854].

5. Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication on the Internet of Healthcare Things. Digital health, 9, p.20552076231177144. [doi: https://doi.org/10.1177%2F20552076231177144].
6. Yaseen, AA, Patel, K, Yassin, A A, Aldarwish, AJ & Hussein, HA. 2023. Secure Electronic Healthcare Record Using Robust Authentication Scheme. IAENG International Journal of Computer Science 50(2). [Online Full Text]
7. Benetti, E, Sapori, S & Mazzini, G., 2023. Adoption of Two-Factor Authentication in a Pre-Existing Heterogeneous System. In 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-6). IEEE. [doi: https://doi.org/10.23919/SoftCOM58365.2023.10271633]
8. Pieterse, H., 2021. The cyber threat landscape in South Africa: A 10-year review. The African Journal of Information and Communication,28, pp.1-21. [doi: 10.23962/10539/32213]
9. Mwim, EN, Mtsweni, J & Chimbo, B. 2023. Factors Associated with Cybersecurity Culture: A Quantitative Study of Public E-health Hospitals in South Africa. In International Symposium on Human Aspects of Information Security and Assurance (pp. 129-142). Cham: Springer Nature Switzerland. [doi: 10.1007/978-3-031-38530-8_11]
10. Singh, A. 2021. Securing the privacy of patients' electronic personal information in South African hospitals during COVID-19 (Doctoral dissertation).
11. Naik, S. 2021. Johannesburg - Several of South Africa's leading hospitals and health-care organisations have been targeted by cyber criminals during the Covid-19 pandemic. Available from: https://www.iol.co.za/saturday-star/news/sa-hospitals-under-further-strain-due-to-increase-in-cyber-attacks-efb62b96-9170-43e9-b1af-475783472ba9 (Accessed 21 March 2024).
12. Verizon Data. 2022. Data Breach Investigations Report on cyber-attacks on South African healthcare. Available from: https://www.verizon.com/business/resources/reports/dbir/ (Accessed 12 March 2024).
13. Cline, GB & Luiz, JM. 2013. Information technology systems in public sector health facilities in developing countries: the case of South Africa. BMC medical informatics and decision making, 13, pp.1-12. [doi: 10.1186/1472-6947-13-13]
14. Apex. 2023. Safeguarding Patient Data: Navigating Cybersecurity Challenges in South Africa's Healthcare Industry. Available online: https://apexcybertechnologies.co.za/blog/safeguarding-patient-data-navigating-cybersecurity-challenges-in-south-africas-healthcare-industry/ (Accessed 12 November 2023)
15. Díaz-López, D Dólera-Tormo, G, Gómez-Mármol, F and MartínezPérez, G 2016. "Dynamic countermeasures for risk-based access control systems: An evolutive approach," Future Generation Computer Systems 55, pp. 321–335. [doi: 10.1016/j.future.2014.10.012]
16. Jayabalan, M. and O'Daniel, T., 2019. A study on authentication factors in electronic health records. Journal of Applied Technology and Innovation 3(1), pp 7-14. [Open Access]
17. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y (2018) Multi-factor authentication: a survey. Cryptography 2(1):1. [doi: 10.3390/cryptography2010001]
18. Thakkar V &Shah V. 2021. Investigation of Techniques used for Mitigating Security and Privacy Issues in Cloud Based Electronic Health Record (EHR) Systems. - International Journal of Innovative Science, Engineering & Technology, 8(2): 466-478. [Open Access]
19. Parkavi, R, Iswarya, MJ, Kirithika, G, Madhumitha, M & Varsha, O. 2023. Data Breach in the Healthcare System: Enhancing Data Security. In Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies (pp. 418-434). IGI Global.
20. Chigada, J. and Madzinga, R., 2021. Cyberattacks and threats during COVID-19: A systematic

literature review. South African Journal of Information Management, 23(1), pp.1-11. [doi: 10.4102/sajim.v23i1.1277]

21. Minnaar, A. and Herbig, F.J., 2021. Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. Acta Criminologica: African Journal of Criminology & Victimology, 34(3), pp.155-185. [doi: 10520/ejc-crim_v34_n3_a10]
22. Olorunju, N. 2019. Data security: the protection of personal health information in the healthcare system. Journal Of Public Administration, 54(3), pp.363-377. [doi: 10520/EJC-1aa9c43aa8]
23. Hermanus, S.S., 2023. Information system security vulnerabilities: Implications for South African financial firms in Cape Town. [Open Access]
24. Letseka, G.T., 2022. *Cybersecurity Readiness in South African Public Sector Organisations* (Doctoral dissertation, University of Johannesburg).
25. Mtsweni, J.S., Shozi, N.A., Matenche, K., Mutemwa, M., Mkhonto, N. and Jansen van Vuuren, J., 2016. Development of a semantic-enabled cybersecurity threat intelligence sharing model. 11th International Conference on Cyber Warfare & Security, 17 - 18 March 2016, Boston University, Boston, USA
26. Chuma, KG & Ngoepe, M. 2022. Security of electronic personal health information in a public hospital in South Africa. Information Security Journal: A Global Perspective, 31(2): 179-195. [doi: 10.1080/19393555.2021.1893410]
27. Mannan, H., McVeigh, J., Amin, M., MacLachlan, M., Swartz, L., Munthali, A. and Van Rooy, G., 2012. Core concepts of human rights and inclusion of vulnerable groups in the disability and rehabilitation policies of Malawi, Namibia, Sudan, and South Africa. Journal of Disability Policy Studies, 23(2), pp.67-81. [doi: 10.1186/1752-4458-7-7]
28. Van Heerden, R., Von Solms, S. and Vorster, J., 2018. Major security incidents since 2014: An African perspective. In 2018 IST-Africa Week Conference (IST-Africa) (pp. Page-1). IEEE. [Open Access]
29. Verizon Data. 2020. Data breach investigations report in South African healthcare. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/ (Accessed 21 May 2023).
30. National Department of Health. 2019. "National Digital Health Strategy for South Africa 2019 - 2024"in better health for all South Africans enabled by person-centered Digital. Retrieved from: [Open Access]
31. Dhillon, PK & Kalra, S. 2018. Multi-factor user authentication scheme for IoT-based healthcare services. Journal of Reliable Intelligent Environments, 4, pp.141-160. [doi: 10.1007/s40860-018-0062-5]
32. Fareed, M & Yassin, AA. 2022. Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system. Bulletin of Electrical Engineering and Informatics, 11(4), pp.2131-2141. [doi: 10.11591/eei.v11i4.3658]
33. Odiango, H.M., Abeka, S. and Liyala, S., 2022. Health information systems security: Risks, prospects and frameworks. World Journal of Advanced Engineering Technology and Sciences, 6(2), pp.057-070. [doi: 10.30574/wjaets.2022.6.2.0082]
34. Els, F. and Cilliers, L., 2017. Improving the information security of personal electronic health records to protect a patient's health information. In 2017 Conference on Information Communication Technology and Society (ICTAS) (pp. 1-6). IEEE. [doi: 10.1109/ICTAS.2017.7920658]
35. Mbunge, E., 2020. Effects of COVID-19 in South African health system and society: An explanatory study. Diabetes & Metabolic Syndrome. Clinical Research & Reviews, 14(6), pp.1809-1814. [Doi: 10.1016/j.dsx.2020.09.016]

36. Tamene, E.H., 2016. Theorizing conceptual framework. Asian Journal of Educational Research Vol, 4(2), pp.50-56. [Open Access]
37. Ravitch, S.M. and Riggan, M., 2016. Reason & rigor: How conceptual frameworks guide research. Sage Publications. [doi: 10.1080/07380577.2017.1360538]
38. Varpio, L, Paradis, E., Uijtdehaage, S. and Young, M., 2020. The distinctions between theory, theoretical framework, and conceptual framework. Academic Medicine, 95(7), pp.989-994. [doi: 10.1097/acm.0000000000003075]
39. Haag, S., Siponen, M. and Liu, F., 2021. Protection motivation theory in information systems security research: A review of the past and a road map for the future. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 52(2), pp.25-67. [doi: 10.1145/3462766.3462770]
40. Khan, NF, Ikram, N, Murtaza, H & Javed, M. 2023. Evaluating protection motivation-based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security, 125, p.103049. [doi: 10.1016/j.cose.2022.103049]
41. Vrhovec, S. and Mihelič, A., 2021. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, 106, p.102309. [doi: 10.1016/j.cose.2021.102309]
42. Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R. and Leukfeldt, E.R., 2023. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security, 127, p.103099. [doi: 10.1016/j.cose.2023.103099]
43. Shillair, R.J., 2018. *Mind the Gap: Perceived Self-Efficacy, Domain Knowledge and Their Effects on Responses to a Cybersecurity Compliance Message* (Doctoral dissertation, Michigan State University).
44. Kumar, D.D., Vijay, K., Bhavani, S., Malathy, E. and Mahadevan, R., 2017. A study on different types of authentication techniques in data security. *International Journal of Civil Engineering and Technology*, *8*(12), pp.194-201. [OpenAccess]
45. Hussain, M., Mehmood, A., Khan, S., Khan, M.A. and Iqbal, Z., 2019. Authentication techniques and methodologies used in wireless body area networks. *Journal of Systems Architecture*, *101*, p.101655. [doi: 10.1016/j.sysarc.2019.101655]
46. Purkayastha, S., Goyal, S., Oluwalade, B., Phillips, T., Wu, H. and Zou, X., 2021. Usability and security of different authentication methods for an electronic health records system. arXiv preprint arXiv:2102.11849. [doi: 10.48550/arXiv.2102.11849]
47. Segun, O.F. and Olawale, F.B., 2017. Healthcare data breaches: Biometric technology to the rescue. *Int. Res. J. Eng. Technol*, *4*(11), pp.946-950. [Open Access]
48. Kwao, L, Xornam Ativi, W., Hayfron-Acquah, J.B. and Panford, J.K. 2019. User Authentication Model for Securing E-Health System using Fingerprint Biometrics. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 7. [doi: https://dx.doi.org/10.2139/ssrn.3673596]
49. Shahi, S., Redestowicz, M. and Costadopoulos, N., 2020. Authentication in E-health services. In 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA) (pp. 1-10). IEEE. [doi: 10.1109/CITISIA50690.2020.9371820]
50. Tipton, S.J., Forkey, S. and Choi, Y.B., 2016. Toward proper authentication methods in electronic medical record access compliant to HIPAA and CIA triangle. Journal of medical systems, 40, pp.1-8. [doi: 10.1007/s10916-016-0465-x]
51. Bhartiya, S. and Mehrotra, D. 2013. Threats and challenges to security of electronic health records. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th*

International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers 9 (pp. 543-559). Springer Berlin Heidelberg. [doi: 10.1007/978-3-642-37949-9_48]

52. Hamed, N.M. and Yassin, A.A., 2022. A Secure and Authentication Scheme to Preserve the Privacy of Electronic Health Records in the Healthcare System. In 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT) (pp. 32-37). IEEE.Iannone E, Guadagni R, Ferrucci F, De Lucia A, Palomba F (2022) The secret life of software vulnerabilities: a large-scale empirical study. IEEE Trans Software Eng 1. [doi: 10.1109/TSE.2022.3140868].
53. Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M. and García-Berná, J.A., 2024. Security vulnerabilities in healthcare: an analysis of medical devices and software. Medical & Biological Engineering & Computing, 62(1), pp.257-273. [doi: 10.1007/s11517-023-02912-0]
54. Reddy, J., 2021. *Data breaches in healthcare security systems* (Master's thesis, University of Cincinnati).
55. Esther Omolara, A., Jantan, A., Abiodun, O.I., Arshad, H., Dada, K.V. and Emmanuel, E., 2020. HoneyDetails: A prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. *Health informatics journal*, *26*(3), pp.2083-2104. [doi: 10.1177/1460458219894479]
56. Kumar, P., Lee, S.G. and Lee, H.J., 2011. A user authentication for healthcare application using wireless medical sensor networks. In *2011 IEEE International Conference on High Performance Computing and Communications* (pp. 647-652). IEEE. [doi: 10.1109/HPCC.2011.92]
57. Anusuya, T. and Mohamed, ES. 2018. Cybercrime and Cyber Security Issues and Challenges on Healthcare: A Survey. Indian Journal of Engineering, Science, and Technology, 8(1): 23. [Open Access]
58. Bensahab, L., Abouelmehdi, K. and Elmoutaouakkil, A., 2023. Protecting Patient Privacy: Understanding and Classifying Attacks and Vulnerabilities in Web-Based Healthcare Records. In International Conference on Advanced Intelligent Systems for Sustainable Development (pp. 315-327). Cham: Springer Nature Switzerland. [doi: 10.1007/978-3-031-52388-5_28]
59. Nidhya, R., Kumar, M., Maheswar, R. and Pavithra, D., 2022. Security and privacy issues in smart healthcare system using internet of things. IoT-Enabled Smart Healthcare Systems, Services and Applications, pp.63-85. [doi: 10.1016/j.cmpbup.2022.100071]
60. Ali, R., Pal, A.K., Kumari, S., Sangaiah, A.K., Li, X. and Wu, F., 2024. An enhanced three factor-based authentication protocol using wireless medical sensor networks for healthcare monitoring. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-22. [doi: 10.1007/s12652-018-1015-9]
61. Austin, A., Smith, B. and Williams, L., 2010. Towards improved security criteria for certification of electronic health record systems. In *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care* (pp. 68-73). [doi: 10.1145/1809085.180909]
62. Smith, B., Austin, A., Brown, M., King, J.T., Lankford, J., Meneely, A. and Williams, L., 2010. Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In Proceedings of the second annual workshop on Security and privacy in medical and home-care systems (1-12). [doi: 10.1145/1866914.1866916]
63. Al-Zubaidie, M., Zhang, Z. and Zhang, J., 2021. User authentication into electronic health record based on reliable lightweight algorithms. In Handbook of Research on Cyber Crime and Information Privacy (pp. 700-738). IGI Global. [Open Access]

64. Hamed, N.M. and Yassin, A.A., 2022. A Secure and Authentication Scheme to Preserve the Privacy of Electronic Health Records in the Healthcare System. In 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT) (pp. 32-37). IEEE.Iannone E, Guadagni R, Ferrucci F, De Lucia A, Palomba F (2022) The secret life of software vulnerabilities: a large-scale empirical study. IEEE Trans Software Eng 1. [doi: 10.1109/TSE.2022.3140868]
65. Eom, G., Byeon, H. and Choi, Y., 2022. Security vulnerabilities analysis of improved user authentication techniques for electronic medical record systems in aging society. Gerontechnology, 21. [doi: 10.4017/gt.2022.21.s.609.pp4]
66. Chinnasamy, P., Deepalakshmi, P. and Shankar, K., 2020. An analysis of security access control on healthcare records in the cloud. In *Intelligent Data Security Solutions for e-Health Applications* (pp. 113-130). Academic Press. [doi: 10.1016/B978-0-12-819511-6.00006-6]
67. Li, Y. and Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, pp.8176-8186. [doi: 10.1016/j.egyr.2021.08.126]
68. Hoffman, S.A.E., 2020. Cybersecurity threats in healthcare organizations: exposing vulnerabilities in the healthcare information infrastructure. World Libraries 24(1). [Open Access]
69. Wasserman, L & Wasserman, Y. 2022. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 4, p.862221. [doi: 10.3389/fdgth.2022.862221]
70. Banerjee, S., Barik, S., Das, D. and Ghosh, U. 2023. EHRs Security and Privacy Aspects: A Systematic Review. In IFIP International Internet of Things Conference (pp. 243-260). Cham: Springer Nature Switzerland. [doi: 10.1007/978-3-031-45878-1_17]
71. Della PD. 2014. In-depth interviews. Methodological practices in social movement research, pp.228-261. [doi: 10.1093/acprof:oso/9780198719571.001.0001]
72. Lo, N.W., Wu, C.Y. and Chuang, Y.H., 2017. An authentication and authorization mechanism for long-term electronic health records management. *Procedia computer science*, *111*, pp.145-153. [doi: 10.1016/j.procs.2017.06.021]
73. Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, pp.74361-74382. [doi: 10.1109/ACCESS.2019.2919982]
74. Frumento, E. 2019. Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution. MHealth current and future applications, pp.35-69. [doi: 10.1007/978-3-030-02182-5_4]
75. Lehto, M, Neittaanmäki, P, Pöyhönen, J & Hummelholm, A. 2022. Cyber security in healthcare systems. In Cyber Security: Critical Infrastructure Protection (pp. 183-215). Cham: Springer International Publishing. [doi: 10.1007/978-3-030-91293-2_8]
76. Agarwal, R & Kumar, M. 2022. Cyber Security for Handling Threats in Healthcare Devices. In Healthcare Systems and Health Informatics (pp. 217-233). CRC Press. [doi: 10.1201/9781003146087]
77. Mehraeen, E, Ayatollahi, H & Ahmadi, M., 2016. Health information security in hospitals: the application of security safeguards. Acta informatica medica 24(1): 47. [doi: 10.5455%2Faim.2016.24.47-50]
78. Fernández-Alemán, JL, Señor, IC, Lozoya, PÁO & Toval, A. 2013. Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics 46(3): 541-562. [doi: 10.1016/j.jbi.2012.12.003]
79. Li, X, Niu, J, Kumari, S, Liao, J, Liang, W & Khan, MK. 2016. A new authentication protocol for

healthcare applications using wireless medical sensor networks with user anonymity. Security and Communication Networks, 9(15): 2643-2655. [doi: 10.1002/sec.1214]

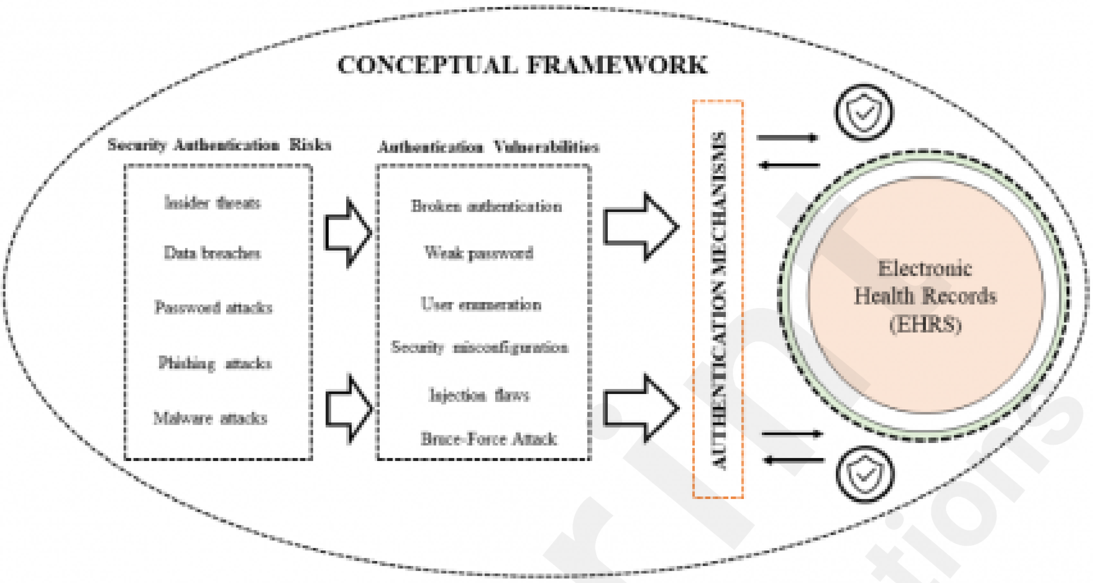
80. Kalyango, S.T. and Maiga, G., 2012. A technique for strengthening weak passwords in electronic medical record systems. In Foundations of Health Informatics Engineering and Systems: First International Symposium, FHIES 2011, Johannesburg, South Africa, August 29-30, 2011. Revised Selected Papers 1 (pp. 207-224). Springer Berlin Heidelberg. [doi: 10.1007/978-3-642-32355-3_13]
81. Quimiz-Moreira, M., Zambrano-Romero, W., Moreira-Zambrano, C., Mendoza-Zambrano, M. and Cedeño-Palma, E., 2021. Cybersecurity mechanisms for information security in patients of public hospitals in Ecuador. In *The International Conference on Advances in Emerging Trends and Technologies* (pp. 211-224). Cham: Springer International Publishing. [doi: 10.1007/978-3-030-96147-3_17]
82. Fauzi, M.A., Yeng, P., Yang, B. and Rachmayani, D., 2021. Examining the link between stress level and cybersecurity practices of hospital staff in Indonesia. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-8). [doi: 10.1145/3465481.3470094]
83. Hepp, S.L., Tarraf, R.C., Birney, A. and Arain, M.A., 2018. Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. Health Information Management Journal, 47(3), pp.116-124. [doi: 10.1177/1833358317722038]
84. Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F. and Griffiths, J., 2020. Privacy, confidentiality, security, and patient safety concerns about electronic health records. International nursing review, 67(2): 218-230. [doi: 10.1111/inr.12585]
85. Latulipe, C, Mazumder, SF, Wilson, RK, Talton, JW, Bertoni, AG, Quandt, SA, Arcury, TA. & Miller, DP. 2020. Security and privacy risks associated with adult patient portal accounts in US hospitals. JAMA internal medicine 180(6), pp.845-849. [doi: 10.1001/jamainternmed.2020.0515]
86. Dekker, MAC & Etalle, S. 2007. Audit-based access control for electronic health records. Electronic Notes in Theoretical Computer Science, 168(1): 221–236. [doi: 10.1016/j.entcs.2006.08.028]

Supplementary Files

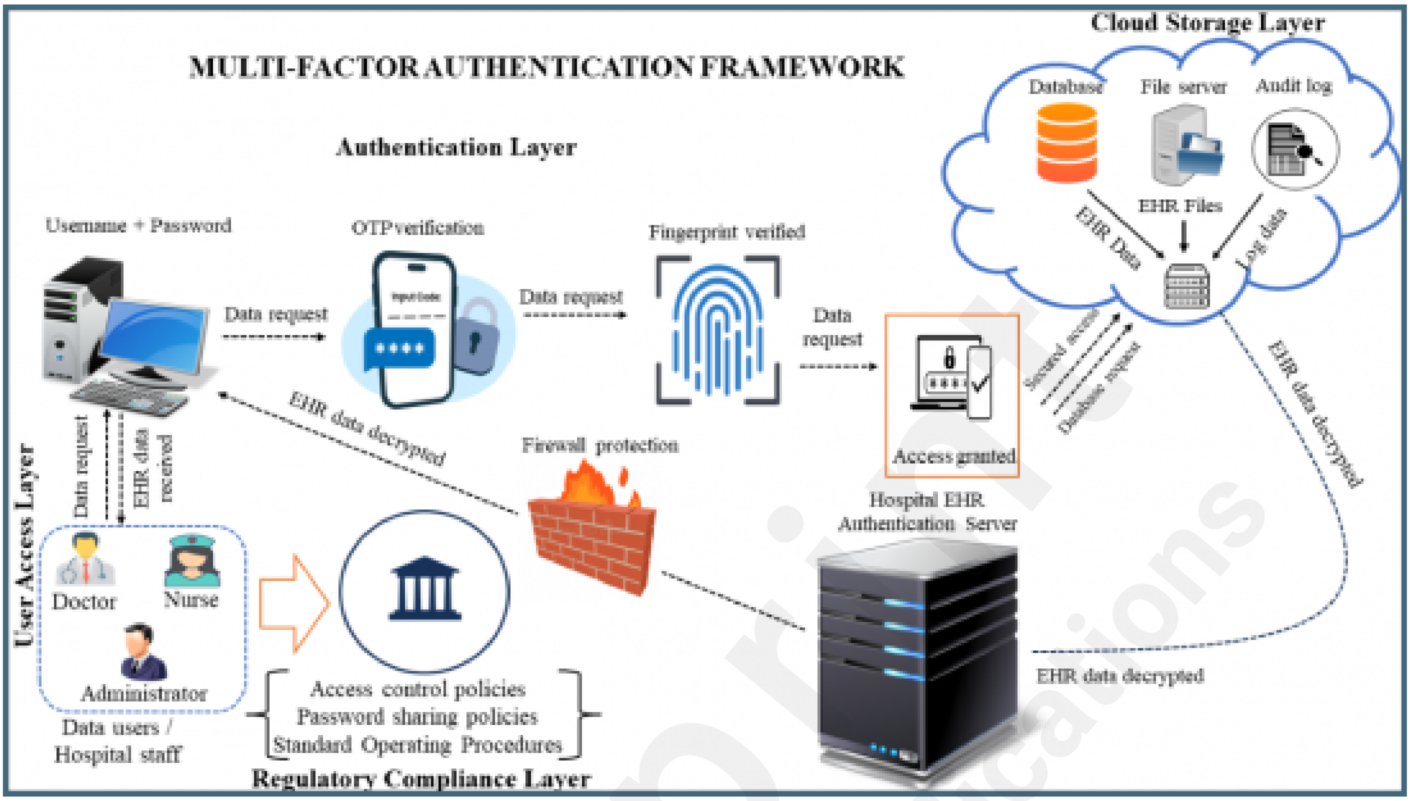
Untitled.
URL: http://asset.jmir.pub/assets/2195e47f84c57125a4e693f0c22a1a7a.docx

Figures

Conceptual framework.



Framework for integrating MFA.


MULTI-FACTOR AUTHENTICATION FRAMEWORK
Authentication Layer
Cloud Storage Layer
Database
File server
Audit log
EHR Files
EHR Data
Log data
Username + Password
OTP verification
Fingerprint verified
Data request
Data request
Data request
Access granted
Secured access
Database request
EHR data decrypted
Firewall protection
Hospital EHR Authentication Server
EHR data decrypted
EHR data decrypted
Data request
EHR data received
User Access Layer
Doctor
Nurse
Administrator
Data users / Hospital staff
Access control policies
Password sharing policies
Standard Operating Procedures
Regulatory Compliance Layer