Vol. 8, No. 1, February 2026

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Post-Quantum Cryptography for securing Electronic Health Records in the South African Public Healthcare System

Kabelo Given Chuma[1]

[1,]Department of Information Science, College of Human Science, University of South Africa

Received:
December 26,, 2025
Revised:
January 1, 2026
Accepted:
January 28, 2026
Published:
March 7, 2026

Corresponding Author:
Author Name*:
Kabelo Given Chuma
Email*:
chumakg@unisa.ac.za

DOI:
10.63158/journalisi.v8i1.1423

Abstract. The growing dependency on Electronic Health Records (EHRs) has intensified the exposure of sensitive patient information to advanced cybersecurity threats, including those posed by quantum computing technologies. South African public hospitals depend on conventional encryption mechanisms to secure EHRs; however, these methods are susceptible to quantum threats. The study explored quantum-resistant cryptography for securing EHRs in South African healthcare. The study adopted a phenomenological approach, employing semi-structured interviews with 12 ICT specialists, policymakers, health information managers and cybersecurity practitioners. The study established a misalignment between national digital health and cybersecurity strategies and future quantum threats, as they prioritise digital transformation, data security and interoperability. Public hospitals were found to be reliant on conventional encryption methods, resulting in structural lock-in and impeding adaptability of post-quantum cryptography. Although stakeholders demonstrated awareness of quantum threats, organisational readiness remains constrained by technical, institutional and capacity barriers. It is concluded that South African public healthcare system remains behind towards post-quantum security transformation. The study recommends the development of a roadmap for post-quantum cryptographic migration, system modernisations and capacity building to strengthen the security of EHRs. The findings provide evidence-based guidance for policymakers to strengthen digital health security and resilience of EHRs in public healthcare systems.

Keywords: Electronic Health Records, Post-Quantum Cryptography, Quantum Computing Threats, Cybersecurity Policy, South African Public Healthcare

1. INTRODUCTION

The digitalisation of health system has significantly transformed the healthcare industry, making clinical operations more efficient and transformed how patient information is collected, managed and used to provide care. [1] underscore that the landscape of healthcare has undergone a transformative shift from paper-based records to electronic health records (EHRs). As a consequence, this transition has been a cornerstone for boosting efficiency and enhancing patient outcomes. [2] stresses that EHRs are backbone to contemporary healthcare by enabling rapid access to patient records, which supports more accurate diagnoses, individualised care plans, and enhanced overall patient outcomes. However, this digital shift has increased the arena for cyber actors and hackers to exploit vulnerabilities in rapidly adopted health systems and misuse patient healthcare information for personal benefits.

[3], [4] attest that the growing dependency on increasingly complex digital health systems and platforms have intensified the exposure of sensitive patient information to increasingly sophisticated cybersecurity threats and attacks. Due to the sensitive nature of the information contained in EHRs, the healthcare sector remains the prime target for cyber incidents, including phishing attacks, data breaches, ransomware and other cybercrimes. Beyond these conventional security threats, [5] advocate the view that the convergence of quantum computing introduces substantial threats and disruptive risks to existing cryptographic encryptions such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC), that are widely used in many healthcare facilities worldwide. In support of this position, [6] further substantiate that traditional cryptographic algorithms used to protect sensitive data in EHRs are increasingly susceptible to quantum-based threats, particularly those enabled by Shor's and Grover's algorithms.

Likewise, the primary weakness of these conventional encryption techniques is that their security relies on the assumption that classical computers cannot feasibly break the encryption without the correct key. Building on this concern, [7] contend that emerging quantum computers that use quantum bits to perform complex computations at exponentially faster speeds, pose significant and immediate threat to the conventional encryption techniques currently safeguarding EHRs in hospitals. In response, this looming threat has placed significant pressure on global authorities such as the World Health Organisation (WHO), the United States National Institute of Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA), the National Cyber Security Centre (NCSC) and the Centers for Disease Control and Prevention (CDC) to prioritise the transition to quantum-resistant cryptographic techniques, which have the potential to withstand quantum threats and attacks.

[8], [9] emphasise that healthcare facilities at various levels must proactively transition to quantum-resistant cryptographic algorithms before quantum computing threats attain the capability to compromise existing encryptions used in EHRs. Given this context, [10], [11], [12] stress critical infrastructures such as government ministries and departments, national security agencies, healthcare facilities and financial institutions in developed countries such as United States, Netherlands, Germany and Australia have begun implementing roadmap, programs and workforce development initiatives for post-quantum cryptography (PQC) migration. In a similar manner, Canadian healthcare organisations and government agencies are prioritising multi-layered security models that integrate PQC with classical encryption to create hybrid digital systems capable of protecting sensitive data against the looming threats posed by quantum computing [13], [14].

Despite growing awareness and substantial investments in PQC initiatives across Europe and North America, the vast majority of African countries continue to lag behind in establishing dedicated quantum initiatives. At the same time, [15], [16] underscore that low- and middle-income countries (LMICs) such as Nigeria, India, Rwanda and Pakistan remain significantly behind in terms of digital infrastructure, policy development and large-scale migration strategies to accelerate the shift from conventional encryption methods to new PQC encryption standards. Although, several initiatives aimed at strengthening digital health security in Africa, like the Union Digital Transformation Strategy (2020-2030), the National Cybersecurity Strategy (2024), the eHealth Strategy Framework and the Smart Africa Digital Health Agenda have been introduced, progress towards migration from traditional cryptographic systems to PQC algorithms remains limited.

[17], [18] assert that many healthcare services across Egypt, the Middle East, and North Africa have long relied on fragmented and misaligned digital health systems, legacy infrastructure, outdated software and traditional encryption algorithms such as RSA, ECC and AES (Advanced Encryption Standard). As a consequence, EHRs across the continent remain susceptible not only to evolving cybersecurity threats but also to quantum computing threats. Critically, across the Africa, no country has made efforts towards initiating a national post-quantum migration strategy and very limited conceptual studies examined quantum-resistant cryptography within the healthcare context, revealing a significant policy and research gap.

Given this context, South Africa like most Africa countries has made considerable progress towards leveraging EHRs to improve efficiency, quality and patient safety. Unfortunately, many of these systems depend on classical cryptographic primitives such as RSA, AES and ECC, alongside outdated authentication mechanisms and legacy software, making them particularly susceptible to future quantum-enabled attacks that could compromise large volumes of stored or transmitted health data. In support of this concern, [19], [20] assert that most South Africa public hospitals, clinics and other community services rely solely on public-key cryptography algorithms such as RSA, AES, and ECC, which, although secure against current classical computers, are increasingly threatened by advances in quantum computing. Furthermore, the South Africa government has demonstrated commitment to digital health through national frameworks such as the National Digital Health Strategy (2019–2024), the National Health Insurance (NHI), National eHealth Strategy (2012–2016) and the National e-Government Strategy [21].

However, while these national frameworks prioritise digital health interventions, including data interoperability, eHealth, data exchange and progress towards the Universal Health Coverage (UHC), they fall shot in addressing emerging quantum computing threats and attacks, resulting in notable gaps in national security preparedness. As a consequence, the absence of a defined national post-quantum migration strategy exposes the South African healthcare system to future quantum attacks, presenting a significant gap for policymakers, regulators and regulatory bodies responsible for protecting sensitive patient information. Another noticeable gap is that, although there is abundant literature on quantum-resistant cryptography for securing EHRs; however most of these studies are conceptual analysis and have been conducted in developed countries like United Kingdom, Australia, and Germany.

Therefore, there is lack of empirical study that addresses cryptographic readiness in South African and African context. This study sought to bridge the policy and empirical gap by exploring the integration of quantum-resistant cryptography for securing EHRs in the South African public healthcare system, with a view to propose recommendations to strengthen preparedness for quantum computing threats. To achieve this, the study was guided by the following research objectives:

1) Determine whether existing national digital health frameworks address emerging quantum computing threats to EHRs in the South African public healthcare system
2) Assess existing cryptographic security mechanisms used to protect EHRs in South African public healthcare system
3) Ascertain healthcare stakeholders' perceptions and understanding of quantum computing threats to EHRs in the South African public healthcare system
4) Identify barriers affecting the adoption of quantum resistant cryptography in the South African public healthcare system
5) Propose recommendations to strengthen preparedness for quantum computing to EHRs in the South African public healthcare system

By addressing these research objectives, this study makes substantial contribution to the literature on digital health security. This study provides empirical evidence from the South African public health system relating to cryptographic and preparedness for post-quantum security readiness, addressing the research gap in the existing body of knowledge dominated by conceptual studies in developed countries. This study offers an analysis of policy readiness through examining the extend to which national digital health and cybersecurity frameworks respond to emerging PQC threats. Furthermore, the study identified structural lock-in barriers such as legacy systems, institutional constraints and limited technical capabilities that hinder the adoption of PQC in public healthcare. Overall, this study contributes to a holistic understanding of PQC readiness in resource constraints health systems and inform policy and strategic planning.

2. METHODS

The researcher followed a systematic procedure when conducting this study. Firstly, the researcher began this study by reviewing the relevant literature on PQC in healthcare to establish the research problem and identify the knowledge gaps and formulate the research objectives. This was followed by selecting the appropriate research methodology to ensure that accurate and relevant methods and techniques are used to collect data to understand the phenomenon under investigation. In the next stage, researcher conducted semi-structured interviews with participants working in the public healthcare system.

This allowed reflexibility while ensuring alignment with the research objectives. As a follow up, the research began with analysing the data using thematic analysis, involving combination of inductive and deductive coding to identify recurring patterns and theoretically informed constructs. Lastly the researcher interpreted the emerging themes and synthesised them to formulate the study findings. Figure 1 illustrates the sequential methodological procedure followed in this study.

The study adopted an interpretive (Heideggerian) phenomenological approach to understand the perceptions, experiences and insights of experts and stakeholders with regards cryptographic security practices and preparedness of post-quantum threats in the public healthcare system. Unlike a case study, which is limited to bounded organisational settings, phenomenology enabled the researcher to explore shared meanings across multiple institutional levels, including technical, policy and governance levels. Therefore, phenomenology was considered the most suitable design to understand how stakeholders perceive, experience and respond to emerging post-quantum cryptographic threats within complex healthcare environment.

The study recruited experts working in various levels of the health system, from the national policy level to provincial ICT and cybersecurity management. This enabled the researcher to gain diverse insights and perspectives from different functional levels across the healthcare system. Participants were purposively sampled, including policymakers, ICT specialists, health information managers and cybersecurity practitioners. Eligibility criteria for participation in this study included participants who had at least 5 to 15 years of executive or managerial experience and knowledge in security of health information systems. Despite extensive expertise in health ICT and cybersecurity, none of the participants was a specialist in post-quantum cryptography, which may have influenced the depth of technical knowledge.

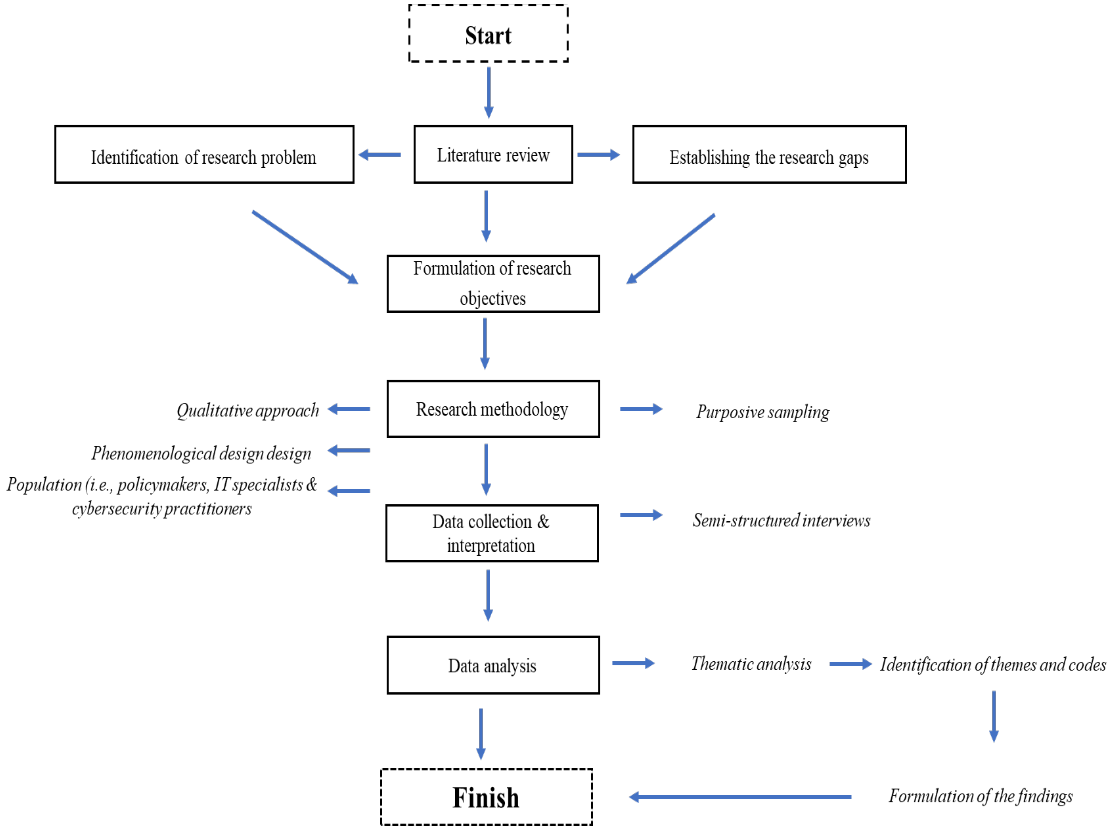
Start
Identification of research problem
Literature review
Establishing the research gaps
Formulation of research objectives
Qualitative approach
Research methodology
Purposive sampling
Phenomenological design design
Population (i.e., policymakers, IT specialists & cybersecurity practitioners
Data collection & interpretation
Semi-structured interviews
Data analysis
Thematic analysis
Identification of themes and codes
Finish
Formulation of the findings

Figure 1. Sequential methodological procedure

Study participants were approached via email and face-to-face interactions in their respective offices and through MS Teams and telephone. Interviews were conducted with Twelve (12) participants. In total, six interviews were conducted in person, four via MS Teams and two through telephone call. Data were collected from January to March 2025. A semi-structured interview guide with open-ended questions was used to collect data from participants through face to face and via MS Teams.

The interview guide was developed based on the objectives of this study. The interview questions were piloted with three healthcare experts to assess their clarity and to determine whether the questions were relevant or require revisions. Upon reviewing the initial data collected, minor changes were made to the original data collection instrument. All interviews were conducted in English and digitally recorded (with permission) to ensure accuracy and integrity of the collected data. These recordings were complemented by field notes taken during the interviews. Each interview session lasted approximately 45 minutes and continued until data saturation. To ensure transparency in this study, the following questions were asked: what cryptographic mechanisms used to protect EHRs in your public institution? How prepared do you think South African public healthcare system is for quantum computing threats to EHRs? and barriers affecting the adoption of quantum resistant cryptography for EHRs? These questions were used to allow probing and clarification based on participants responses.

Data saturation was achieved by the 9th participant. The extra three participants were added to ensure depth of the collected data. The sample size was considered adequate for a phenomenological study, where depth of insight is prioritised over breadth, and data saturation is used as the criterion for determining sample adequacy. The interviews were transcribed verbatim and transcripts were sent to participants for accuracy and validation. Any personal identifiable information was redacted in transcripts to maintain confidentiality and privacy.

Data were analysed thematically following the steps proposed by [22]. A familiarization process was undertaken by reading the transcripts repeatedly, followed by inductive coding based on the participants' narratives, as well as deductive coding based on existing literature regarding EHR security and post-quantum cryptography. Based on constant comparisons across the dataset, related codes were grouped into categories. A review of the final themes was conducted to ensure that they were coherent and distinctive, and they were validated by the members. Atlas.ti 24 was used to facilitate systematic coding, audit trails, and theme refinement.

To gain a deeper understanding of the data, the interview transcripts were reviewed multiple times. The researcher applied an inductive, data-driven coding approach, where initial codes were generated based on the common themes and meanings that emerged from the data. Using an iterative process of constant comparison, related codes were clustered and categorized into provisional themes. Subsequently, these themes were viewed across the entire dataset, refined for internal consistency and distinctiveness, and clearly articulated as recurring patterns among the participants.

In this study, the trustworthiness was achieved through several qualitative measures, including credibility, dependability, confirmability, and transferability [23]. Credibility of the data was ensured through member checking, in which participants were provided with an opportunity to review and confirm the findings to ensure accuracy. Dependability and confirmability were ensured through maintaining an audit trail of coding and iterative theme refinement within ATLAS.ti. Moreover, transferability was ensured through documenting a clear research process using an audit trail

This study was reviewed and approved by the College of Human Science Research Ethics Committee of the University of South Africa (HREC Ref number: #4353) and was conducted according to the Declaration of Helsinki. All participants provided written and verbal informed consent prior to the commencement of interviews, and data were anonymized to protect participant confidentiality. All interviews were carried out on a voluntary basis and participants could withdraw from the study at any stage. No participant approached refused to participate or withdraw from the study. Data collection and storage procedures adhered to the requirements of the General Data Protection Regulation (GDPR). Moreover, transcripts were anonymised and securely stored in a computer system with password and username, with access restricted to authorised members of the research team only.

3. RESULTS AND DISCUSSION

3.1. Demographic characteristics of the participants

The study sample comprised of 12 participants, including policymakers, ICT specialists, health information managers and cybersecurity practitioners. The professional experience of the participants ranged from 6 to 28 years. Their highest academic qualifications ranged from the National Diploma to a Masters' Degree. The demographic characteristics of the participants are presented in Table 1.

Table 1. Demographic characteristics of the participants

Pseudonyms	Professional category	Qualification	Experience
HC-1	Policymaker	Bachelor's Degree	15 Years
HC-2	ICT Specialist	National Diploma	8 Years
HC-3	Cybersecurity Practitioner	Honours Degree	12 Years
HC-4	Policymaker	Master's Degree	25 Years
HC-5	ICT Specialist	Bachelor's Degree	10 Years
HC-6	Health Information Manager	Master's Degree	18 Years
HC-7	Cybersecurity Practitioner	Honours Degree	11 Years
HC-8	Health Information Manager	Doctoral Degree	28 Years
HC-9	Policymaker	Bachelor's Degree	9 Years
HC-10	ICT Specialist	Honours Degree	6 Years
HC-11	Cybersecurity Practitioner	Master's Degree	15 Years
HC-12	ICT Specialist	National Diploma	10 Years

Source: Research Data (2025)

The following Table 2 presents the themes, categories and sub-categories

Table 2. Themes, Categories and Sub-categories

Themes	Categories	Sub-categories
1. National digital health framework for quantum era health security	1.1 Absence of quantum-focused policy direction	• No reference to quantum computing threats in national digital health frameworks
	1.2 Short-term policy orientation	• Emphasis on immediate digital transformation goals • Limited future-orientated cybersecurity foresight
2. Cryptographic security mechanisms used to protect EHRs	2.1 Reliance on classical encryption standards	• Continued reliance on RSA, ECC and AES • Dependence on public-key cryptography designed for classical computing

Themes	Categories	Sub-categories
	2.2 Structural lock-in of legacy systems	• Deep integration of conventional encryption into EHRs architecture • Limited adaptability of existing health information systems
	2.3 Vulnerability of current cryptographic assumptions	• Expected breakdown of RSA and ECC under quantum attacks • Invalidation of classical threats models
	2.4 Long-term confidentiality risk	• Data decryption threats • Extended retention periods of patient records
3. Stakeholders' perceptions and understanding of quantum computing threats to EHRs	3.1 Recognition of quantum risks	• Perception of quantum computing as a disruptive cybersecurity force • Awareness of implications for patient privacy
	3.2 Limited operational preparedness	• Awareness not translated into actionable planning • Absence of concrete implementation roadmaps
4. Barriers to the adoption of quantum resistant cryptography for EHRs	4.1 Technical and infrastructural barriers	• Incompatibility of legacy systems with quantum resistant algorithms • Complex system upgrade requirements
	4.2 Financial barriers	• High cost of software and hardware • Competing budgetary priorities in hospitals
	4.3 Organisational and governance barriers	• Lack of institutional readiness and leadership priorities. • Centralised decision-making and bureaucratic delays
	4.4 Human capacity limitations	• Shortage of PQC expertise

Source: Research Data (2025)

The following Figure 2 illustrate the relationship between themes, categories and codes

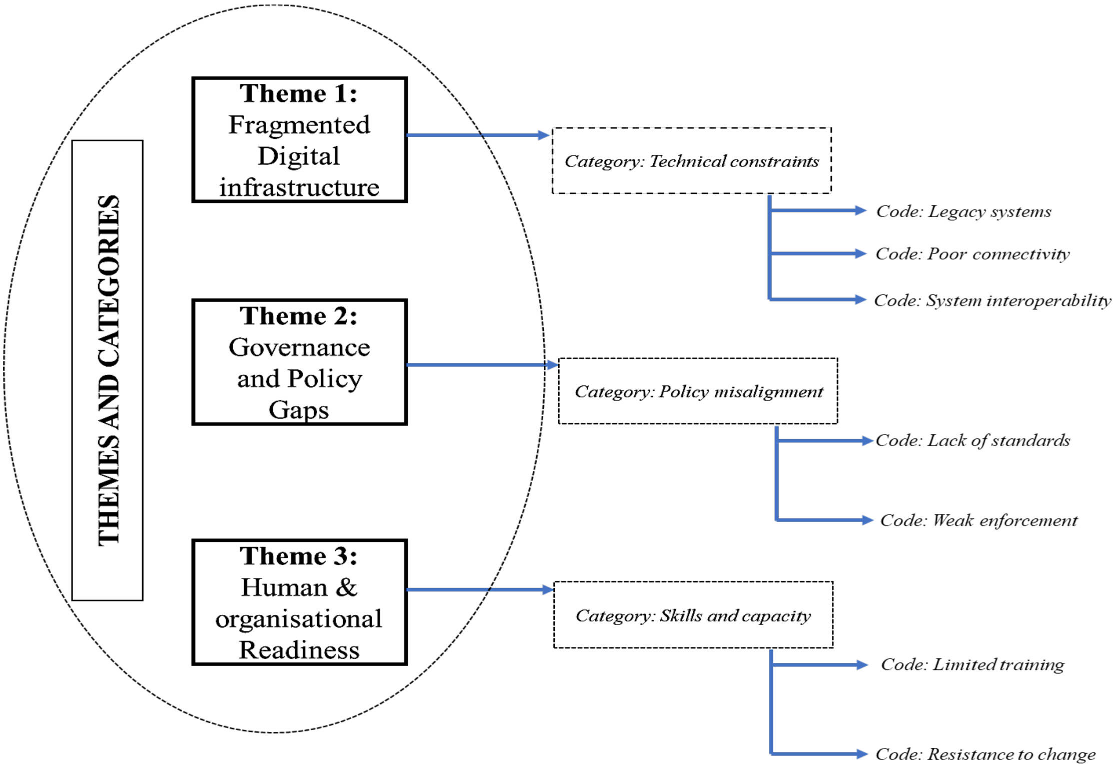
THEMES AND CATEGORIES
Theme 1: Fragmented Digital infrastructure
Theme 2: Governance and Policy Gaps
Theme 3: Human & organisational Readiness
Category: Technical constraints
Code: Legacy systems
Code: Poor connectivity
Code: System interoperability
Category: Policy misalignment
Code: Lack of standards
Code: Weak enforcement
Category: Skills and capacity
Code: Limited training
Code: Resistance to change

Figure 2. The relationship between themes

3.2. National digital health frameworks for addressing quantum computing threats

Participants emphasised that current frameworks prioritise digital transformation, interoperability, and general data protection, fall short in addressing emerging quantum computing threats. For instance, participants responded as follows:

Absence of quantum-focused policy direction

One of the participants said: *"the existing national frameworks that we have in South Africa, such as the National Digital Health Strategy of 2019-2024 and National e-Government Portal Strategy are mainly focused on enabling digital transformations, system integration and data exchange; however, they do not consider future risks and threats such as quantum computing" (HC-4).* Another participant similarly noted that *"national strategies place strong emphasis on strengthening integrated health information systems and cybersecurity in a very general sense such as protecting patient health data and ensuring secure*

EHRs. They fail to address conventional encryptions that are currently used in public healthcare facilities and anticipate quantum enabled threats or post quantum migration" (HC-7)

Short-term policy orientation

One of the participants mentioned that *"most national digital health documents we have in South Africa were drafted before quantum computing became a major concern in the field of cybersecurity. Due to this, they place a greater emphasis on modernization of health information systems as opposed to anticipating future cryptographic threats" (HC-5).* Another participant offered similar sentiments that: *"in South Africa most of national policies and frameworks prioritise aspects such as interoperability and standards, digital health adoption, and privacy and security and overlook future issues like protecting computer systems and EHRs against next generation threats, including quantum computing" (HC-10)*

3.3. Cryptographic security mechanisms for protecting EHRs

All the participants expressed that hospitals continue to reliant on traditional cryptographic algorithms like AES, ECC and RSA to secure patient health information. For example:

Reliance on classical encryption standards

One of the participants said: *"Most of the healthcare systems I have worked with, legacy encryption methods, such as RSA and ECC, are used to ensure the confidentiality of patient records and data exchange between systems" (HC-3).* Another participant similarly indicated that *"EHR security architecture is still based on conversational or legacy encryption standards like AES, ECC and RSA. These classical cryptographic mechanisms remain the backbone for protecting patient health data in most of our public hospitals...I think this is because they are well understood and already integrated into most existing systems. So, the South African public healthcare system should make every effort transition to cryptographic models that are resilient to emerging quantum threats" (HC-12).*

Structural lock-in of legacy systems

> One of the participants indicated that *"most of our hospitals and clinics in South Africa are still relying heavily on classical cryptographic encryptions such as RSA and ECC for protecting patient records. The issue is that these algorithms were design for classical computing environment and they not been re-designed or evaluated against future quantum related threats" (HC-11)*

As a follow up question, participants mentioned several security concerns relating to these mechanisms. For examples:

Vulnerability of current cryptographic assumption

> One of the participants said: *"biggest concern with these traditional algorithms is that they may no longer viable in the next coming years when quantum threats become practical in South Africa. Therefore…this means that the data that is encrypted in our systems today could potentially be decrypted and exploited by third parties like cybercriminals or hackers" (HC-2).* Another participants offered a similar response that: *"the most significant weaknesses of these cryptographic systems is that they assume that attackers will only be able to employ classical computing power. It is anticipated that the security assumptions underlying our current EHR systems will be invalidated once quantum computing reaches maturity" (HC-8)*

Long-term confidentiality risks

> Another participant indicated that *"One of the greatest challenges I foresee with these conventional encryptions is the lifespan of our health records. Even if ECC and RSA are deemed to be more secure today, but patient data stored for decades may be harvested and decrypted when quantum capabilities become available" (HC-9)*

3.4. Stakeholders' perceptions and understanding of quantum computing threats to EHRs

Participants in the interviews perceived quantum computing as a significant future risks to the cryptographic foundations currently used in hospitals to secure EHRs. For instance, participants expressed the following views:

Recognition of quantum risks

One of the participants said: *"Despite the fact that quantum computing is still emerging, I have a strong believe it represents a serious challenge to the encryption techniques currently used to secure electronic health records, particularly public-key cryptography" (HC-1).* Similarly, another participant said: *"there is a high possibility that quantum computing could break widely used encryption algorithms like RSA and ECC, which would have serious implications for patient confidentiality and privacy" (HC-5).* Moreover, another participant indicated that *"I am concerned not only about quantum attacks happening immediately, but about the possibility that patient information stored today could be decrypted in the future, which creates long-term risks for patient privacy" (HC-8)*

Limited operational preparedness

In contrast, another participant offered a different response *"As far as cybersecurity is concerned, quantum computing represents a paradigm shift. I think in the absence of comprehensive planning or clear roadmaps, patient health data that is stored in EHRs could be compromised retrospectively as soon as quantum capabilities become available" (HC-6)*

3.5. Barriers affecting the adoption of quantum resistant cryptography for EHRs

Participants mentioned a range of technical, financial and organisational barriers that could hinder the implementation of quantum resistant cryptography solution for securing EHRs in public sector hospitals. For example:

Financial constraints

One of the participants said *"cost implications are among the major barriers toward implementing quantum resistant cryptography. Because, this technology requires new hardware, specialised software and continuous system upgrades and our public hospitals are already struggling with limited budget and financial resources that barely cover basic operational needs" (HC-8)*

Technical and infrastructural barriers

Another participant offered a different response *"most of our existing health information system and EHRs are particularly built on legacy encryption standards…so they are not compatible with quantum resistant algorithms. So, because of this, upgrading or modernising our systems would require more changes to digital infrastructure, software and interoperability protocols, which currently our government and public hospitals do not have the capacity to implement" (HC-1)*

Organisational and governance barriers

One of the participants indicated that *"The major barrier is that there is a lack of institutional readiness and strategic planning around post-quantum security among our public hospitals…At an organisational level, quantum threats are not a matter or urgent or immediate priority but there is no clear roadmap or policy guiding the readiness towards adopting quantum-resistant cryptography for protecting patients' records" (HC-9).* Another participant similarly noted *"The main barrier is that the there is a high degree of centralisation and slowness in the public health care system. It is a fact that, even when technical teams identify the need for stronger cryptography solutions, bureaucracy and fragmented governance will delay the approval and implementation of these technologies" (HC-12)*

Human capacity limitations

One of the participants offered a different response and said *"My concern is the lack of skilled personnel who are familiar with quantum-resistant cryptography. Despite the fact that most IT staff in public healthcare facilities receive conventional cybersecurity training, there is little support for training in emerging cryptographic technologies" (HC-5).*

3.6. Discussion

This section discusses the results of this study. The findings of this study indicate a significant misalignment between existing national frameworks for digital health and cybersecurity frameworks in South Africa and the emerging risks of quantum computing in the healthcare industry. Participants consistently perceived that current frameworks place an emphasis on immediate priorities such as digital transformation, systems integration and data protection, with little consideration given to future-oriented cryptographic risks. Despite that these health frameworks intended to strengthen the health information systems and protect patient data, the are perceived as insufficient forward-looking, particularly considering the potential disruption that quantum technologies could potentially bring to existing encryption mechanisms.

As a result of this short-term policy orientation, many of these frameworks were developed during a period in which quantum computing was not widely recognised as an imminent threat the healthcare cybersecurity. Thus, this results in a little strategic direction at the national level concerning post-quantum readiness, cryptographic migration or long-term data security in the South African healthcare. The findings further revealed that South African public sector hospitals are still predominantly using classical cryptographic algorithms such as AES, RSA and ECC for the security of EHRs. This finding is consistent with prior studies by [19], [24], [25] who stressed that a growing number of hospitals and healthcare organisations are still reliant on legacy systems, which use traditional algorithms and technologies, coexisting with modern systems that make them susceptible to cyberattacks.

Nonetheless, the mechanisms are highly integrated in health information systems and have become the default approach due to their maturity, widespread acceptance and integration into existing infrastructures. However, this reliance causes a structural lock-in within cryptographic system architectures, making adaption to emerging cryptographic paradigms complex and costly. Participants expressed concerns that these algorithms have not been re-evaluated in the context of quantum computing capabilities, thereby increasing the risk of future compromise of healthcare data. Furthermore, study participants expressed significant weakness in the assumptions underlying current cryptographic due to this reliance on conventional encryption. The findings indicate that these security mechanisms assume adversaries are limited to classical computational power, an assumption that may no longer be valid in the near future.

Participants expressed concerns regarding the long-term confidentiality of healthcare records due to their prolonged retention period. Moreover, participants perceived quantum computing as a future threat and paradigm shift that could weaken the cryptographic foundations of existing EHRs in public sector hospitals. The findings of this study support those of [26], [27], [28] who stipulated that the emergence of quantum computing presents a serious long-term threat to the confidentiality of healthcare data encrypted using traditional methods. The results showed that the absence of clear roadmaps, national guidance and implementation limit the efforts of public hospitals to migrate to post-quantum cryptography.

The findings further revealed that the practical adoption of quantum-resistant cryptographic is South African public sector hospitals remain constrained by various challenges. It is evident from the findings of this study that limited financial resources restrict the ability of hospital to invest in new cryptographic methods, whereas legacy health systems coupled with outdated infrastructure limit technical flexibility for post-quantum migration. These issues are further compounded by a shortage of personnel with expertise in post-quantum cryptography. As a result of these barriers, it is evident that while quantum computing presents several potential risks, substantial systemic, institutional, and capacity-related challenges must be addressed before quantum-resistant cryptographic solutions can realistically be implemented in South African public healthcare settings.

Globally, South African situation reflects those of many African countries where digital health initiatives have grown rapidly but remain reliant on legacy infrastructure and conventional cryptographic models. Similar challenges have been reported in Nigeria, Rwanda, and Egypt, where limited financial resources, fragmented governance, and a shortage of skills hinder the adoption of advanced cybersecurity measures. As a result of its more mature digital health frameworks and national cybersecurity strategies, South Africa is considered to be in a better position than many other countries. In this regard, the country is well positioned to become a regional leader in the area of post-quantum preparedness if proactive policies are implemented, capacity building is conducted, and systems are modernized. Overall, the study demonstrates that post-quantum cryptographic readiness is not a technical issue but a systemic challenge requiring coordinated policy action, institutional reform, and long-term investment.

This study proposes the following recommendations to strengthen preparedness for quantum computing threats in the protection of EHRs in South African public healthcare:

1) **Long -term recommendations (3 to 10 years)**
   a) The government should develop a comprehensive national roadmap to guide public sector hospitals in transitioning from traditional cryptographic algorithms to quantum-resistant cryptographic algorithms. The roadmap should be strictly aligned with international standards for post-quantum to ensure interoperability and prioritises high-risk systems like EHRs and outlines timeframe for cryptographic audits.
   b) A sufficient budget should be allocated to support post-quantum security initiatives in public healthcare. Parallel to this, governance structures should to be strengthened to enhance the partnership between healthcare, cybersecurity, and digital transformation authorities to reduce bureaucratic delays, and improve decision-making for quantum-resistant cryptography.
   c) Public hospitals should devote the necessary resources to develop a modernisation strategy to reduce structural lock-in. It is important for this strategy to introduce crypto-agile architectures, enabling modular upgrades, and ensuring that modern health information systems procured by the public health sector can support quantum-resistant cryptography.

2) **Short-term recommendations (1 to 3 years)**
   a) The South African government in collaboration with the National Department of Health should revise the digital health and cybersecurity frameworks to address future quantum computing threats. They must incorporate clear guidelines on long-term data security, cryptographic migration and quantum readiness in the national digital health strategy and cybersecurity policies.
   b) Healthcare stakeholders should establish a comprehensive capacity building program to address the skills gaps and needs identified within scope of quantum cryptography. This may include training for IT personnel, partnerships with universities and research institutions, and continuous professional development programs directed at emerging cryptographic technologies.

4. CONCLUSION

This study explored the integration of quantum-resistant cryptography for securing EHRs in the South African public healthcare system. The findings of the present study demonstrate that while conventional cryptographic methods remain effective in the short term, they are deemed to be ineffective for ensuring the long-term confidentiality, integrity and privacy of sensitive health data. The results confirmed a strong dependence on traditional cryptographic approaches within public sector hospitals, alongside with fragmented policy frameworks and legacy system infrastructure, which exposes them to future quantum computing security threats and risks. In response to the research objective, the study established that the South African healthcare system remain strategically unprepared for post-quantum computing security transformation. Despite the growing awareness among health stakeholders regarding quantum computing security threats, this awareness has not been translated into strategic migration plan, policy actions or technical preparedness. Due to this, the security of long-term EHRs continues to be at risk beyond current cryptographic capabilities. The study makes valuable contribution towards digital health resilience discourse by introducing PQC readiness as a critical aspect of long-term EHRs security in South African healthcare. The findings of this study offer transferable insights beyond the South African context for other developing countries that are experiencing similar challenges in aligning digital health transformation with emerging cryptographic threats.

This study has several limitations to address. The qualitative and interpretive phenomenological approach used in this study focused on gaining insights rather than achieving broad applicability, making the results specific to the context of the South African public healthcare system. Moreover, participants were chosen from various fields such as policy, ICT, health information management, and cybersecurity, and the study did not involve experts in post-quantum cryptography or perform technical assessments of cryptographic algorithms. As a result, the findings reflect issues related to institutional preparedness, governance, and implementation rather than focusing on cryptographic efficiency or the feasibility of algorithms. Future research could address these limitations through combining qualitative and institutional analysis with technical evaluation of PQC algorithms. They could broaden empirical research to encompass various healthcare systems and regional settings. In line with these conclusions, the study underscores a pressing call to action for policymakers, government and other healthcare authorities to incorporate PQC into national digital health and cybersecurity strategies and policies. In order to ensure long-term future-proof protection of EHRs in public sector hospitals, strategic migration plan, capacity building and alignment with policy and governance must be prioritised. It is recommended that future research be conducted to empirically test feasibility and performance of post-cryptographic algorithms in healthcare setting and propose security frameworks to support robust and secure digital health ecosystem in South Africa

REFERENCES

[1] M. K. Hossain, J. Sutanto, P. W. Handayani, A. A. Haryanto, J. Bhowmik, and V. Frings-Hessami, "An exploratory study of electronic medical record implementation and recordkeeping culture: The case of hospitals in Indonesia," *BMC Health Services Research*, vol. 25, no. 1, pp. 1–20, 2025, doi: 10.1186/s12913-025-12399-0.

[2] R. Margam, "The importance of EHR in revolutionizing healthcare delivery and financial success," *Int. J. Comput. Trends Technol.*, vol. 71, pp. 52–55, 2023, doi: 10.14445/22312803/IJCTT-V71I7P108.

[3] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, "Cybersecurity and cybercrime: Current trends and threats," *Journal of International Studies*, vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[4] S. Gupta, M. Kapoor, and S. K. Debnath, "Cybersecurity risks and threats in healthcare," in *Artificial Intelligence-Enabled Security for Healthcare Systems: Safeguarding Patient Data and Improving Services*. Cham, Switzerland: Springer Nature, 2025, pp. 39–64, doi: 10.1007/978-3-031-82810-2_3.

[5] O. J. Tiwo *et al.*, "Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 187–208, 2025, doi: 10.9734/ajrcos/2025/v18i4615.

[6] T. Anuradha *et al.*, "Quantum-resilient framework for healthcare data security using multivariate polynomial cryptography," *International Journal of System Assurance Engineering and Management*, pp. 1–12, 2025, doi: 10.1007/s13198-025-02954-7.

[7] A. S. Ashour and D. Koundal, "Quantum computing in Healthcare 5.0," in *Quantum Computing for Healthcare Data*. Amsterdam, Netherlands: Academic Press, 2025, pp. 43–62, doi: 10.1016/B978-0-443-29297-2.00009-5.

[8] S. Chahar, "Exploring the future trends of cryptography," in *Next Generation Mechanisms for Data Encryption*. Boca Raton, FL, USA: CRC Press, 2024, pp. 234–257.

[9] M. SaberiKamarposhti *et al.*, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, no. 10, 2024.

[10] E. P. Nittala, "Design and evaluation of quantum-resilient cryptographic protocols for national information systems security," *Int. J. Emerging Trends Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 132–142, 2024, doi: 10.55248/gengpi.6.0425.1586.

[11] A. Alif, K. F. Hasan, J. Laeuchli, and M. J. M. Chowdhury, "Quantum threat in healthcare IoT: Challenges and mitigation strategies," *arXiv preprint*, arXiv:2412.05904, 2024, doi: 10.48550/arXiv.2412.05904.

[12] C. K. Gitonga, "The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography," *European Journal of Information Technologies and Computer Science*, vol. 5, no. 1, pp. 1–10, 2025, doi: 10.24018/ejcompute.2025.5.1.146.

[13] B. Kwame and M. Isabella, "Advancing secure communications: The role of post-quantum cryptography in a digital era," *International Journal of Informatics and Data Science Research*, vol. 1, no. 11, pp. 30–50, 2024.

[14] K. Csenkey and A. Graver, "Canada's national quantum strategy one year on," *Canadian Foreign Policy Journal*, vol. 30, no. 3, pp. 295–306, 2024, doi: 10.1080/11926422.2024.2397970.

[15] A. R. Olatunde and O. I. Olope, "Exploring the evolving threats and future directions of cyber security in the age of technologies," *Int. J. Advances Eng. Manage.*, vol. 6, no. 1, pp. 489–498, 2024, doi: 10.35629/5252-0609489498.

[16] G. Dogbanya *et al.*, "Quantum health policy readiness: Anticipating the next digital disruption in public health," *Journal of Life Science and Public Health*, vol. 1, no. 2, pp. 1–7, 2025, doi: 10.69739/jlsph.v1i2.966.

[17] Z. Lin, "Implementation of de novo FAIRification in relational legacy systems: The case of the electronic medical record system for maternal health in Afya.ke," *FAIR Data, FAIR Africa, FAIR World*, p. 429, 2025, doi: 10.5281/zenodo.15382966.

[18] T. Okasha, N. M. Shaker, and D. A. El-Gabry, "Mental health services in Egypt, the Middle East, and North Africa," *International Review of Psychiatry*, vol. 37, nos. 3–4, pp. 306–314, 2025, doi: 10.1080/09540261.2024.2400143.

[19] K. G. Chuma, "Legacy electronic health record systems as culprit behind cybersecurity risks in public healthcare facilities of South Africa," *Global Security: Health, Science and Policy*, vol. 10, no. 1, p. 2532556, 2025, doi: 10.1080/23779497.2025.2532556.

[20] M. H. Khumalo and T. S. Moloi, "Barriers to digital transformation in Gauteng's municipal health clinics," *Journal of Local Government Research and Innovation*, vol. 6, p. 282, 2025, doi: 10.4102/jolgri.v6i0.282.

[21] K. G. Chuma and M. Ngoepe, "Data interoperability of health information systems in public hospitals in the Gauteng province of South Africa," *Insights into Regional Development*, vol. 7, no. 4, pp. 84–101, 2025, doi: 10.70132/z6986464949.

[22] V. Braun and V. Clarke, "Conceptual and design thinking for thematic analysis," *Qualitative Psychology*, vol. 9, no. 1, pp. 3–26, 2022, doi: 10.1037/qup0000196.

[23] R. H. Adler, "Trustworthiness in qualitative research," *Journal of Human Lactation*, vol. 38, no. 4, pp. 598–602, 2022, doi: 10.1177/08903344221116620.

[24] G. S. Lawal, "Post-quantum cryptography for protecting long-term medical data archives," 2020, doi: 10.13140/RG.2.2.31914.89281.

[25] M. Adil *et al.*, "Quantum computing and the future of healthcare internet of things security: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 12, no. 22, 2025, doi: 10.1109/JIOT.2025.3605040.

[26] A. O. Ezeogu, "Post-quantum cryptography for healthcare: Future-proofing population health databases against quantum computing threats," *Research Corridor Journal of Engineering Science*, vol. 2, no. 1, pp. 29–56, 2025.

[27] M. P. Singh *et al.*, "Impact and implications of quantum computing on blockchain-based electronic health record systems," *The Open Bioinformatics Journal*, vol. 17, no. 1, pp. 1–15, 2024, doi: 10.2174/0118750362316814240820051945.

[28] H. Joshi, "Quantum computing in health informatics: Enhancing disaster preparedness," in *The Rise of Quantum Computing in Industry 6.0 Towards Sustainability*. Cham, Switzerland: Springer, 2024, pp. 101–121, doi: 10.1007/978-3-031-73350-5_7.