RESEARCH-ARTICLE

Challenges and Risks of Digitalizing Health Systems- A Review for South African eHealth

STHEMBILE NTSHANGASE, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

OYENA MAHLASELA, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

MAMELLO MTSHALI, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

UNARINE MANARI, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

LEHLOGONOLO P I LEDWABA, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

MATSHIDISO MARENGWA, The Council for Scientific and Industrial Research, Pretoria, Gauteng, South Africa

Open Access Support provided by:

The Council for Scientific and Industrial Research

Published: 26 November 2025

Citation in BibTeX format

icABCD 2025: 2025 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems
November 26 - 27, 2025
Cape Town, South Africa

https://doi.org/10.1145/3759023.3759121
ISBN: 9798400714276

Challenges and Risks of Digitalizing Health Systems- A Review for South African eHealth

Sthembile Ntshangase*
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
SMlambo@csir.co.za

Oyena Mahlasela
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
omahlasela@csir.co.za

Mamello Mtshali
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
Mmtshali3@csir.co.za

Unarine Manari
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
umanari@csir.co.za

Lehlogonolo P.I.Ledwaba
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
lledwaba4@csir.co.za

Matshidiso Marengwa
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
mmarengwa@csir.co.za

Abstract

This study represents a comprehensive literature review aimed at identifying the challenges and risks associated with the digitalization of health systems. The objective was to assess which healthcare systems are utilized globally and in South Africa. The key digital health systems identified include healthcare management systems, telemedicine, mHealth, electronic health records, cloud, data analytics, wearables, and emerging technologies such as 3D bioprinting, artificial intelligence, and robotics. Recommendations were formulated to promote a balanced approach to health systems digitalization, emphasizing maximizing benefits while mitigating risks and addressing challenges. The recommendations were developed following a review of the identified technologies, focusing on associated risks, challenges, and mitigation measures. Although these technologies enhance healthcare services, they encounter challenges including security issues, limited access, and regulatory compliance. The recommendations propose the enhancement of regulations for compliance and security, with future work concentrating on aligning technologies with South African standards to ensure secure adoption. The findings of this study can assist policymakers and system developers within the Department of Health in South Africa in devising healthcare solutions with minimized risks and challenges.

CCS Concepts

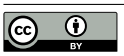
• **Applied Computing**; • **Life and Medical Sciences**; • **Health Care Information Systems**;

Keywords

Digitalization, Healthcare, Digital Health, Electronic Health Record, mHealth

ACM Reference Format:
Sthembile Ntshangase, Oyena Mahlasela, Mamello Mtshali, Unarine Manari, Lehlogonolo P.I.Ledwaba, and Matshidiso Marengwa. 2025. Challenges and Risks of Digitalizing Health Systems- A Review for South African eHealth. In *2025 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD 2025), November 26, 27, 2025, Cape Town, South Africa.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3759023.3759121

*Corresponding Author



icABCD 2025, Cape Town, South Africa

ACM ISBN 979-8-4007-1427-6/2025/11
https://doi.org/10.1145/3759023.3759121

1 Introduction

The combination of data, information systems, communications and medical care is changing how different organizations provide services, including different sectors such as the healthcare industry [1]. There is a rapid growth in the replacement of traditional health services and systems by digitalized services that are driven by technology [2]. This move provides several benefits, such as effectively storing, sharing and accessing health records anytime and anywhere [3]. In addition, technology enables the storage, processing, analysis, faster transfer and accessibility of large amounts of healthcare data, which promotes the productivity of healthcare. Furthermore, through technology medication is securely stored, accessed and managed, likewise, simplified and effective communication between healthcare providers. However, there are risks, challenges and compliance concerns that are introduced by the adoption of these technologies [4]. As healthcare technologies encompass sensitive and personally identifiable information to be stored, shared and accessed, individuals and government are concerned about the availability, confidentiality, safety and privacy of their information [5].

In addition, cybercrime has become a significant threat to the healthcare sector [6]. Research indicates a high rise in cyber-attacks globally that target the healthcare sector. The central, most severe and persistent threat that healthcare must deal with is ransomware,

which is a malware attack that denies user access and usability of healthcare data, files, devices, networks or systems until the ransom payment has been made [7]. The effect of these cyberattacks can be very critical and cost the lives of individuals since they can lead to the inability to perform and complete hospital operations and delay treatments and procedures. Thus, it is very important to understand possible risks, challenges, and cyber-attacks associated with every technology that healthcare is using or adopting to put in place appropriate security controls. Moreover, healthcare technology allows both patients and healthcare providers to access medical information easily. As the world increasingly adopts digital identities, digital wallets, and self-sovereign digital identities, integrating healthcare details into these digital wallets can empower patients to manage their medical information [8]. The South African traditional manual systems can be inconvenient, especially in urgent situations, as patients might have multiple records across different healthcare facilities [9]. This problem can hinder consistent treatment. By incorporating technology, a single, unified medical record can be created for each patient, which they can share and grant access to as needed.

This research identifies and assesses technologies used in the healthcare sector based on the associated benefits, risks, challenges and mitigations. The contribution of this research is to provide South African policymakers, researchers, and healthcare professionals with information on what they need to consider when adopting such technologies. In addition, security considerations are required to develop a healthcare system.

Research questions that are answered during this study are as follows:

- What are current technologies used in healthcare globally and in South Africa?
- What challenges and risks are involved?
- What are the mitigation strategies for identified risks?

The structure of this paper is as follows: Section 1 is the introduction, followed by methodology Section 2. Then, a comprehensive literature on the components of digitalized healthcare is presented in Section 3. Section 4 highlights legislation and regulation. Then, the conclusion is section 5.

2 Methodology

This study adopted a Most Similar Systems Design (MSSD) comparative approach to analyze the effectiveness of digital health systems in South Africa. The MSSD provides a comparison of similar cases, but they may differ in the outcome [10]. The comparison focuses on dimensions such as data privacy policies, interoperability standards, and accessibility of digital health tools, as illustrated in Figure 1. The search term included ("Digitalization Healthcare", OR "Digital Health" OR "Electronic", OR "mHealth"). The academic databases that were used included Scopus, IEEE Xplore and other academic databases and government reports on digital health system initiatives. A thematic analysis was conducted to identify patterns and differences in policy implementation on digitalized healthcare tools. Furthermore, a narrative comparison of each case was analyzed to highlight the contextual factors that determined the outcomes. To ensure validity, data were triangulated from multiple sources. This included but was not limited to policy documents, literature reviews and digital health reports. Moreover, reliability was maintained by using standardized data collection tools and consistent criteria across cases. The limitation of this comparative method is that the findings from the healthcare digitalization tools may only apply to specific or similar systems being compared. Furthermore, there is a risk of oversimplifying contextual nuances as digital health infrastructure may vary drastically in different countries, and this may influence the insight in terms of external validity of the study.

3 digitalization of healthcare

Healthcare Management Systems (HMS) within the eHealth (the usage of information and technologies within the health care sector) space are implemented for planning, organizing, and monitoring care programs and services across a healthcare system [11]. These systems involve the coordination of hospitals, physicians, and resources to provide high-quality care to patients and it is crucial for medical professionals to make informed decisions based on patient history, medical records, and available resources [12]. It is also important in public health, where underserved communities need to manage budgets and resources effectively. Health systems managers assess the need for health services and budgets, make policy recommendations, implement health education programs, integrate healthcare services and technological advancements, collaborate with healthcare professionals, and manage medical records. Healthcare services face three waves of intervention: quality management, risk management, and patient safety [9].

With the rapid growth in the integration of healthcare into nearly every aspect of our lives, the risks for individuals and organizations are increasing. Risks in healthcare include medical malpractice, patient complaints, Health Insurance Portability and Accountability Act (HIPAA) and Protection of Personal Information Act (POPIA) violations, data breaches, and medical accidents [13]. Quality issues pose the most significant risk to healthcare employers, such as ineffective procedures and medical negligence. Thus, implementing and adopting an HMS faces several human and technical challenges [14]. The three main human-related challenges include a shortage of professional healthcare trainers with knowledge and experience of HMS in general. Secondly, there is a low acceptance rate of technologies in healthcare. Thirdly, there is a lack of health informatics professionals who are responsible for governing the establishment and implementation of HMS. Technical challenges with the implementation of an HMS include network and computer maintenance problems, a lack of standards for data entry and retrieval, and difficulties in technically upskilling and training users to use HMS.

To overcome these challenges, it is important to develop a governance model that will ensure that commercial providers and vendors offer proper user manuals, documentation, troubleshooting, and guidelines for HMS use while ensuring compliance with cybersecurity requirements [15]. The important requirement is to ensure security, including ensuring the working conditions of computers and networks, upgrading communication networks and computers, and performing thorough analysis before the design and implementation phases. Additionally, new innovative hardware and software implementations are required to ensure there is no gap caused by

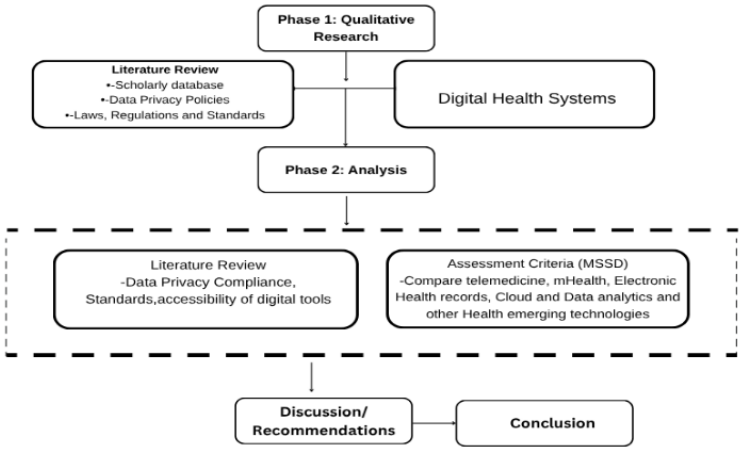


Figure 1: Summary of Comparative Study Methodology

the advancement in technology [16]. All other systems and technologies developed in the healthcare sector are generated based on the management system. The rest of this document discusses the risks and challenges caused by introducing different technologies in the healthcare sector, such as Telemedicine, mHealth, Electronic Health Record, and cloud computing and data analytics.

3.1 Telemedicine

Telemedicine involves the healthcare delivery service and facilitating communication between patients and healthcare providers using advancements in technology [15]. This technology makes use of computers, tablets, or smartphones to enable communication between healthcare providers and patients through video calls, phone calls, etc., and to implement e-prescribing, Service Provider Registry, Health Information Exchange, and mHealth services. These technologies can provide services that include diagnosing and treating medical conditions, medication management, and disease screening. Telemedicine is linked directly to clinical services that provide and apply approved models like chronic care management and remote patient monitoring to effectively ensure that patients with diagnosed health conditions are managed [16].

It is a challenge for traditional manual methods to manage patients' information, prescriptions, and deliver patients' medication on time. Therefore, telemedicine assists by enabling better long-term care management and patient satisfaction. Through this technology, patients can access medical care virtually, especially when transport to medical centers is a challenge or costly to the patient. Although most patients and healthcare providers have not yet adopted telemedicine, it has the potential to significantly impact the future of healthcare. While revolutionary in remote patient care, telemedicine introduces challenges and risks to healthcare providers and patients and how medical appointments operate [1]. Ethical and legal challenges are critical in telemedicine and should be considered when implementing and using telemedicine programs. Furthermore, individuals may require medical support from different locations. Which can be a challenge since healthcare providers, laws, and regulations may differ depending on the location. The implementation of telemedicine involves navigating complex ethical and legal issues [13]. Global authorities have established informed consent requirements to protect patients' awareness of privacy and procedures, which are critical to telemedicine training policies. Despite the complexity and length of the legal framework, a comprehensive understanding is possible, with advancements relying on a thorough assessment of existing laws and regulations.

3.2 mHealth

Mobile Health (mHealth) refers to the application of mobile technologies, including smartphones, patient monitoring equipment, personal digital health assistants, and related devices, to provide support for patients and technical assistance to healthcare professionals [17]. Since its increased usage after COVID-19, mHealth applications improve the overall patient care by enabling health systems and providers to acquire and utilize health information in a simplified manner. In addition, it provides increased and efficient accessibility to different kinds of healthcare services, even to patients who are difficult or take longer to reach. Moreover, the security side of these technologies is that they can store encrypted records and sensitive data of patients, to ensure that relevant patient data can be securely and easily accessed.

It is important to understand that mHealth is mainly utilized for delivering health information to healthcare providers and researchers, while telemedicine is about improving and streamlining the delivery systems in the healthcare industry [15]. The common specific features used for mHealth include monitoring of drug dosage, diagnostic and clinical decision making. Though there are risks and challenges introduced by the adoption and usage of mHealth. The challenges and risks are also affected by different factors such as discipline and type of activities engaged, location where mHealth is being utilized, and level of education for the user. These include insufficient connectivity and infrastructure, scarcity and inadequacy of data, restricted access to essential equipment and devices, and the lack of locally developed applications customized for the South African context [18]. Therefore, there is a need to

provide awareness of relevant regulations to ensure that the usage of mHealth does not put patients' data and health information at risk.

3.3 Electronic Health Records

Paper records have been an administrative burden for health professionals and their assistants [19]. Electronic Health Records (EHRs) represent a potentially transformative approach to enhancing information management, healthcare delivery, and quality of care that could contribute to improved patient outcomes and reduced financial strain [20]. Furthermore, EHRs could increase security for health services through more accurate and up-to-date record keeping, ensuring that healthcare providers are kept liable for providing efficient services. This could also assist during healthcare-related investigations, as all evidence will be kept on record.

However, EHRs should be used with high care as ensuring the privacy and security of healthcare data is very important [21]. In the healthcare context, privacy would focus on managing who can use and control data while security would focus on protecting data from unauthorized activities such as access, misuse, destruction or relocation [22]. In the current traditional systems, records stored on documents can be easily accessed and modified, which results in weak security and privacy. Digitizing records increases the concerns about the adoption of such systems tenfold specifically relating to the risks and challenges associated with storing health records on local or server databases. These challenges include data availability, confidentiality, security, privacy, errors, data breaches, awareness and training for new systems, ethical issues and third-party/supply chain security.

Addressing these risks requires a robust security policy based on existing information security and privacy standards and frameworks, such as NIST-SP 800-53, NIST SP 800-171, COBIT, ISO 27000 series, NIST-CSF, and CIS Controls [24]. These frameworks and standards can assist in ensuring that the Electronic Record System is implemented in a way that will always be accessible to authorized and authenticated individuals as needed, without compromising privacy. Error management protocols would also need to be implemented as part of the risk and security management plans as EHRs are vulnerable to both system and human errors. Human errors — such as typos, mistakes in patient data capture and results documentation — affect the integrity of healthcare data and need to be managed through adequate staff training in new systems making sure that users comply with the associated regulations, standards and policies. [7]. System errors, such as software design and development flaws, technical issues, automated features, medication issues, user experience errors, login and non-repudiation, would need to be managed through careful system engineering, including security from inception, and a comprehensive change management and decommissioning processes.

3.4 Cloud and Data Analytics

This is about storing, sharing and managing data in the cloud and analyzing it to provide evidence-based services to patients [4]. In the healthcare sector, the importance of big data analytics is on the rise, as it presents opportunities to optimize clinical decision-making and improve resource management. Derived from healthcare records and clinical data, including patient records, disease surveillance, and medical tests, big data analytics, when combined with technological innovations and personalized healthcare, can significantly contribute to the prediction, prevention, management, treatment, and eradication of diseases. Additionally, it supports resource management, research advancement, preventive planning, and epidemic control for governmental agencies, policymakers, and hospitals [25]. The evolution of information and communication technology is driving the shift from physical medical records to Electronic Health Record and Electronic Management Record systems, resulting in a spectacular expansion of data. Healthcare apps, which generate voluminous data from sources like wearable devices and patient-reported outcomes, and in some cases integrate limited social media data such as social influences and public health trends, facilitate the increase of big data in the healthcare domain [26].

The healthcare sector faces numerous challenges, including new disease outbreaks and maintaining optimal operational efficiency [27]. Data mining and analytics have the potential to overcome these challenges through the analysis of authentic medical data for predictive or categorization purposes. However, there are several challenges in dealing with complex data, such as data complexity and heterogeneity, data access and completeness, regulatory and security compliance, and operational and analytical efficiency. One of the biggest hurdles in healthcare data analytics is managing multiple sources of information, which can be challenging due to the spread of medical data across many sources and the need for efficient data storage, preparation, and mining [28]. While interoperability is recognized as a principal strategy for addressing data integration challenges, the lack of interoperability within EHRs hinders the effective application of big data analytics. It is imperative for the healthcare sector to expedite the integration of advanced analytical methodologies, such as predictive analytics, machine learning, and graph analytics, which have surpassed traditional regression-based methods, reflecting advancements achieved in other industries [29]. Furthermore, unstructured medical data poses an additional challenge, necessitating sophisticated techniques in text mining, natural language processing, and image recognition.

Security, privacy, and confidentiality are crucial key elements of a robust healthcare infrastructure, and every stakeholder contributes to the assurance of patient privacy and information security. The HIPAA addresses privacy concerns, but with the escalating amount of healthcare data, data analytics researchers face challenges in ensuring anonymity and avoiding data use or disclosure [29]. Advanced analysis techniques are also needed to address the challenges of aggregating, transforming, and performing analytics on complex data. Including machine learning methods and advanced techniques has shown the ability to process and analyse the volume, velocity, and variety of complex data.

3.5 Wearables

This is about collecting health data, increasing prevention and improving health outcomes for users using devices [9]. Wearable sensors have garnered considerable focus in the healthcare sector due to their capacity to extract therapeutically significant health

data from physiological indicators such as heart rate, blood pressure, and body temperature. Wearable sensor networks comprise a variety of health-related sensors distributed across different regions of the body, each employing distinct criteria for the detection and documentation of symptoms [30]. This capability is vital for the timely intervention and administration of medical care in various diseases and impairments. Wearable sensors, often in the form of smartwatches linked to smartphones, are expected to assist humans in carrying out their health responsibilities in the future. However, these technologies face several challenges, including data collection, data transmission, security and privacy, user acceptance, scalability and interoperability, and resource constraints.

The quality, quantity, and resolution of the data gathered are largely dependent on the wearable device itself, posing a considerable challenge for data collection [26]. Pre-processing raw data is necessary to ensure high-quality labelled data, which often requires specialist knowledge or user assistance. For effective data transmission, an energy-conscious strategy is essential, and utilizing distributed computing can reduce delays by shifting processing to network endpoints [9]. Given that wearables gather sensitive data about user location, activity, and mental health, security and privacy are paramount concerns. The absence of a universal solution underscores the importance of ongoing research and development to enhance these crucial elements.

3.6 Other emerging technologies

Other technologies that are currently used in other health facilities but not fully adopted in South Africa include 3D Bioprinting, Artificial Intelligence (AI), Robotics and Blockchain/DLT.

3.6.1 3D Bioprinting. The 3D Bioprinting technology focuses on printing human-like organs and tissues to enhance patient health. Bioprinting utilizes proteins, living cells, and nutrients as raw materials to generate human tissues for the treatment of diseases, recovery from injuries, and the creation of new organs for transplantation [31]. Even though this technology is still in its infancy in South Africa, there has been notable research in the development of 3D bioprinting led by the Central University of Technology with their MedAdd project, which aimed to reduce over-reliance on imported medical devices by promoting 3D printing to manufacture them locally. Furthermore, the South African government has also recognized the potential of adopting 3D bioprinting and is collaborating with academic institutions and industry players. With over 300 additives, manufacturing 3D printing technology systems that have been locally established.

3.6.2 Artificial Intelligence and Robotics. Artificial Intelligence facilitates healthcare, enhances the precision of diagnoses, and predicts potential high-risk medical situations. Robotic systems contribute to both direct patient care and the upkeep of healthcare facilities [29]. They may also serve as surgical support and aid in delivery and transport tasks. AI and healthcare have significantly improved patient care, enhancing productivity, safety, and quality of treatment. AI analyses and visualises patient data, enhancing healthcare administration. There's a rising trend of healthcare providers and patients employing medical apps and games for remote monitoring and data-driven healthcare. [9]. Artificial intelligence facilitates patient empowerment and encourages a more balanced exchange between physicians and individuals seeking care. The integration of cloud computing and AI expands access to vital health information, while the combination of the Internet of Things with AI-driven technologies enhances the efficiency of healthcare provision. Wearable sensors, utilizing wireless technologies like Bluetooth, Wi-Fi, and the internet, are increasingly incorporated into quality healthcare systems.

3.6.3 Blockchain. The exploration of blockchain technology in healthcare aims to augment the efficiency of managing medical records and processing insurance claims, expedite advancements in clinical and biological research, and enrich the repository of medical and health-related information. This technology holds potential for addressing existing challenges in securing electronic medical records, patient data, and other sensitive information. Blockchain ensures the security and compliance of prescription drugs by providing accurate and immutable records for the supply chain [22]. Blockchain allows for the quick and secure transfer of medical records between healthcare institutions, ensuring accuracy and privacy. It also expedites the verification of medical qualifications, reducing fraud and inaccuracies, and preventing dangerous situations. For investigation purposes, it can provide up-to-date information for medical providers and insurance companies, enhancing interoperability and fraud detection through smart contracts [32]. In addition, it secures data from wearable medical devices, ensuring the accuracy and timeliness of critical medical information. However, like other technologies, Blockchain presents risks and challenges, including data privacy, interoperability, scalability, regulatory compliance, data integrity, cost, adoption, and a shortage of technical expertise. Ensuring data privacy is crucial, as public blockchains can expose sensitive data to unintended parties. Integrating blockchain with current healthcare systems can be convoluted and inflated, while scalability can lead to slower transactions and increased costs. Regulatory compliance is also a challenge, as is data integrity and accuracy when adopting new technologies and managing healthcare records.

4 Discussion and recommendations

This section summarizes identified technologies and associated risks and challenges identified, discusses mitigation strategies and provides recommendations.

4.1 Identified Technologies

Presented in Figure 2 is the list of identified technologies grouped into five categories. These provide a proposed framework of different components and technologies involved in the development of a National Health Management System for South African eHealth Services. It encompasses main elements such as governance, legislation, and health technology systems. Moreover, healthcare technology allows both patients and healthcare providers to access medical information easily. As the world increasingly adopts digital identities, digital wallets, and self-sovereign digital identities, integrating healthcare details into these digital wallets can empower patients

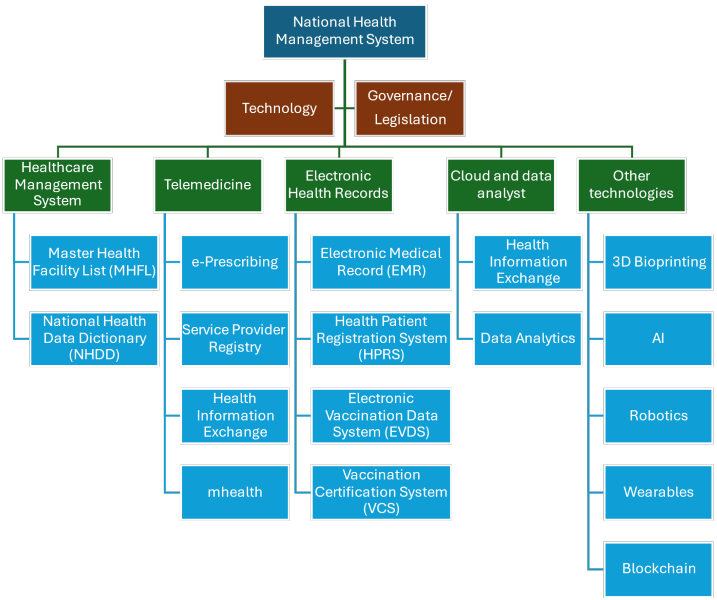


Figure 2: Overall Healthcare Management System.

to manage their medical information [7]. The South African traditional manual systems can be inconvenient, especially in urgent situations, as patients might have multiple records across different healthcare facilities [9] . This problem can hinder consistent treatment. By incorporating technology, a single, unified medical record can be created for each patient, which they can share and grant access to as needed.

Governance or legislation is the main element that assists in managing healthcare systems effectively, while technology covers technological systems and innovations that support healthcare management. South Africa's National Digital Health Strategy [33] already identifies and prioritizes nine strategic interventions covering governance, technology adoption, system interoperability, secure data sharing, implementation and upgrading of healthcare infrastructure, reskilling healthcare workplaces and writing and updating legislation, policies and frameworks surrounding eHealth and their associated management systems [33]. Some components highlighted in the proposed framework have already been undertaken as initiatives by the National Department of Health (NDOH). This includes the development of the Master Health Facility List (MHFL), which is as a comprehensive list of health facilities in South African regions, and the National Health Data Dictionary (NHDD) which is an online, standardized dictionary of health data terms. During the COVID-19 pandemic, the department also issued electronic certificates via the South African COVID-19 Vaccination Certificate System; efficiently and effectively combining records captured at thousands of vaccination centers in both the public and private healthcare system. Give the increasing pressures on the public healthcare system as doctors and nurses struggle to be placed for their com-serve requirements and facilities are understaffed, the use of telemedicine solutions for remote delivery of healthcare services could serve to ease the burden on the system, especially in the rural and more remote communities of South Africa.

Some additional services that could be provided through technology and a National Health Management System include e-Prescribing for chronic illness management, a service provider registry of healthcare service providers within South Africa, from both the public and private sectors for proper distribution of resources in pressurized areas and to facilitate faster com-serve placements of recently graduated healthcare providers, secure health information exchange between different healthcare settings for more complete patient records and comprehensive and tailored treatment plans through e-collaboration with specialists using remote consultation technologies, and mHealth, also called mobile health, is the use of mobile devices to support health services; especially in rural areas where ICT infrastructure may not be as readily available as mobile devices and cellular network connectivity.

4.2 Risks, Challenges and Mitigation Strategies

While the migration to eHealth has the potential for great advantage in the current South African Health sector, there are various risks and challenges that affect the adoption of digital technologies in healthcare which must be considered prior to the adoption of any solution. These have been identified and summarized in Table 1.

Telemedicine and eHealth solutions are vulnerability to data breaches because of the high value of the data being exchanged and the insufficient security measures and training often implemented in healthcare settings. This highlights a need for more efforts and initiatives in establishing stronger security controls related to the protection of healthcare data and systems within South Africa; like the HIPPA Act and its associated security controls.

There is also a limitation in broadband access, especially in rural areas of South Africa, affecting the reach and effectiveness of telemedicine services. While urban areas can access 4G/5G networks, rural communities often have access to 2G/3G networks at best. Developed solutions would need to account for the slower

Table 1: Healthcare Technology: Risks and Mitigation Strategies.

Technology	Risks	Challenge	Mitigation
Telemedicine	Exposure to data breaches is due to the lack of vigorous security controls and national cybersecurity legislation and frameworks.	In South Africa, there is limited broadband access in rural areas. Regulatory and licensing issues make it difficult for new market players to expand connectivity access in South Africa (e.g. Starlink versus ICASA).	Technically, the implementation of end-to-end encryption is essential It is important to establish telemedicine guidelines and standards that will comply with South African regulations and laws.
mHealth	Data privacy concerns third-party applications	Data misuse and unauthorized data access are prevalent in South Africa even after the implementation of the POPIA Act	Implement standardization across mHealth solutions Enforce strict App security audits
Electronic Health Records	Data unavailability, due to technical issues and poor user awareness and training	Ethical issues Third-party/supply chain security Lack of updated government cybersecurity regulations and standards regarding health records in South Africa	Regular reviews and security assessments of the EHR to ensure the system and its usage comply with the related regulations and standards such as NIST-SP 800-53, NIST SP 800-171, COBIT, ISO 27000 series, NIST-CSF, and CIS Controls
Cloud and Data Analytics	Inefficient data handling Large data cloud solutions have storage outside of South Africa	Data complexity and heterogeneity, data access and completeness, regulatory and security compliance and operational and analytical efficiency. Lack of data anonymity and high chances of data misuse.	Considering machine learning methods and advanced techniques to process and analyse the volume, velocity, and variety of complex data. Ensuring compliance with healthcare standards.
Others (Health care emerging technologies)	Lack of risk awareness Slow implementation of strategic plans regarding eHealth	Privacy and information security Outdated strategic and governance plans in terms of global standards for eHealth	Ensuring compliance with South African regulatory bodies and standards can assist in controlling and managing the use of these technologies while ensuring security and preserving privacy.

transfer rates and the security vulnerability associated with the older generation communication protocols. With regulatory and licensing issues presenting a challenge for new market players to enter in the telecommunications space, more consistent implementation and provisioning will be needed in the development of telemedicine services customized for the challenges identified within South Africa's telecommunications spaces with end-to-end encryption prioritised as a mechanism to ensure the security and privacy of patient data and communications. This would be in combination with establishing new policies, guidelines and standards at a national level specifically tailored for telemedicine and eHealth that adhere to South African and International laws and regulations to ensure legal and practical viability.

Data privacy remains a high concern with mobile health (mHealth) applications, particularly those developed by third parties, given the growing misuse of data and unauthorized access to personal information. Given the sensitivity of health information, it is recommended to implement standardization across mHealth solutions, ensuring that consistent privacy and security protocols are in place. This could come in the form SABS standards for mobile health applications and frameworks for assessing the security maturity of mHealth applications, given the stricter security requirements for data privacy and confidentiality. Additionally, enforcing strict security audits for applications can help prevent data breaches and ensure that apps comply with privacy regulations.

Risks associated with the EHR include failure to access data by all healthcare providers, as needed, which can disrupt healthcare services. In South Africa, power failures and other technical problems can further hinder the functionality of EHR systems. Additionally, there is a need for early-stage training and awareness programs for all parties involved when new systems are introduced to ensure smooth integration and operation. Hence, it is recommended that ethical considerations be considered when managing EHRs. Security concerns related to third-party vendors and the supply chain must be addressed to protect sensitive health data, as some of these technologies are imported from other countries. Additionally, regular evaluations of EHR systems are necessary to ensure they are functioning correctly and are compliant with relevant regulations and standards. It is suggested that regulatory compliance should be prioritised by considering related standards and frameworks that serve as guidelines for ensuring EHR systems are secure and compliant with industry best practices.

Identified challenges and considerations related to cloud and data analytics in healthcare data management and analysis include the risk of inefficient data handling. There is a concern over inefficient storage, preparation, and mining of data from various sources, which suggests a need for improved systems to oversee

data more effectively. This is especially concerning with cloud services hosted outside of South Africa where standards governing data management and privacy might differ from what is prescribed by POPIA (for better or for worse). Given the complexity and diversity of healthcare data, assessing authorised access, retrieving and integrating data from different formats and sources and validating completeness remain ongoing challenges, especially in instances where the physical source material itself may have been incomplete. In addition, there are concerns over the lack of data anonymity and the risk of misuse, highlighting the need for establishing security measures to protect sensitive information. It is recommended to use machine learning and advanced analytics to manage and understand the large, fast-moving, and varied data while also ensuring compliance with critical healthcare industry standards and regulations like HIPAA, which safeguard patient information.

5 Conclusion and Future Work

While the integration of digital technologies into healthcare offers substantial advantages, it also introduces complex risks and challenges. Identified technologies that are considered in South Africa include Telemedicine, mHealth, Electronic Health Record, Cloud and Data Analytics and Wearables. Other technologies are still at a very early stage of consideration such as Artificial Intelligence and Robotics Health Systems, 3D Bioprinting and Blockchain-based storage management. Telemedicine in South Africa faces key challenges such as data breaches due to insufficient security, limited broadband access in rural areas, and difficulties in regulatory compliance. The lack of physical examination capabilities further complicates accurate diagnoses. Recommendations include implementing end-to-end encryption, establishing guidelines to adhere to local laws, and standardizing mHealth solutions to manage data privacy. Concerns with EHRs encompass data access, technical disruptions, and the need for training and ethical management, requiring regular system evaluations and compliance with global standards. Cloud and data analytics present risks like inefficient data handling and compliance with legal standards, prompting the use of machine learning for better data management. Wearable technologies raise privacy concerns over data collection and storage, necessitating adherence to regulatory standards to protect user information. Future work includes identifying South African regulations and standards and assessing these technologies against the requirements of those standards and laws, to ensure compliance, security and non-repudiation during the adoption of these technologies.

Acknowledgments

This work was supported in part by the Council for Scientific and Industrial Research (CSIR) and the National Department of Health (NDOH). The findings and conclusions are solely those of the authors and cannot be attributed to the CSIR or NDOH.

References

[1] G. Sannino, G. De Pietro, and L. Verde, "Healthcare Systems: An Overview of the Most Important Aspects of Current and Future m-Health Applications," Connected Health in Smart Cities, pp. 213–231, Jan. 2020, doi: 10.1007/978-3-030-27844-1_11.

[2] "UNO Technologies - 5 benefits of technology in healthcare." Accessed: Sep. 20, 2024. [Online]. Available: https://www.unotech.io/5-benefits-of-technology-in-healthcare

[3] "Why Is Technology Important In Healthcare - WheelHouse IT." Accessed: Sep. 20, 2024. [Online]. Available: https://www.wheelhouseit.com/why-is-technology-important-in-healthcare/

[4] V. Shah1 and S. Reddy, "Cloud Computing in Healthcare: Opportunities, Risks, and Compliance," Conseio Superior De Investigaciones Cientificas, vol. 16, no. 03, pp. 50–70, Apr. 2022, doi: 10.5281/zenodo.10779522.

[5] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," BMC Med Inform Decis Mak, vol. 20, no. 1, pp. 1–10, Jul. 2020, doi: 10.1186/S12911-020-01161-7/PEER-REVIEW.

[6] C. Tredger, "Cyber crime a major threat to SA's healthcare sector | ITWeb," ITWeb. Accessed: Sep. 20, 2024. [Online]. Available: https://www.itweb.co.za/article/cyber-crime-a-major-threat-to-sas-healthcare-sector/P3gQ2MGABYPvnRD1

[7] Smile ID, "2024 Digital Identity Fraud in Africa Report," 2024.

[8] I. Popela, T. Zuva, and M. Appiah, "Factors That Influence the Adoption of Electronic Patients Records Management Systems in South Africa," Proceedings - 2019 International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2019, Nov. 2019, doi: 10.1109/IMITEC45504.2019.9015918.

[9] N. Kostyshak, "Healthcare Management System (HMS): Features and Benefits," Otakoyi Software. Accessed: Oct. 15, 2024. [Online]. Available: https://otakoyi.software/blog/healthcare-management-system-features-and-benefits.

[10] C. Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research," Int J Soc Res Methodol, vol. 11, no. 5, pp. 389–401, Dec. 2008, doi: 10.1080/13645570701401552.

[11] C. Staunton, R. Adams, L. Horn, and M. Labuschaigne, "A Framework to Govern the Use of Health Data for Research in Africa: A South African Perspective," Philosophy and Medicine, vol. 132, pp. 485–499, 2023, doi: 10.1007/978-3-031-12692-5_26.

[12] N. Makeleni and L. Cilliers, "Critical success factors to improve data quality of electronic medical records in public healthcare institutions," SA Journal of Information Management, vol. 23, no. 1, Mar. 2021, doi: 10.4102/SAJIM.V23I1.1230.

[13] A. Laullchander, "The perceived role of digitisation of electronic health records in South African hospitals," University of the Witwatersrand, Johannesburg, 2023.

[14] WHO, "WHO Global Model Regulatory Framework for medical devices including in vitro diagnostic medical devices, Annex 3," World Health Organization. Accessed: Oct. 15, 2024. [Online]. Available: https://www.who.int/publications/m/item/who-global-model-regulatory-framework-for-medical-devices-including-in-vitro-diagnostic-medical-devices--annex-3

[15] G. Nittari *et al.*, "Telemedicine Practice: Review of the Current Ethical and Legal Challenges," Telemedicine and e-Health, vol. 26, no. 12, pp. 1427–1437, Dec. 2020, doi: 10.1089/TMJ.2019.0158/ASSET/IMAGES/TMJ.2019.0158_FIGURE1.JPG.

[16] ASTP/ONC|HealthIT.Gov, "Laws, Regulation, and Policy | HealthIT.gov," Assistant Secretary for Technology Policy/Office of the National Coordinator | HealthIT.Gov. Accessed: Oct. 16, 2024. [Online]. Available: https://www.healthit.gov/topic/laws-regulation-and-policy

[17] H. Noorbhai and T. A. Ojo, "mHealth and e-Learning in health sciences curricula: a South African study of health sciences staff perspectives on utilisation, constraints and future possibilities," BMC Med Educ, vol. 23, no. 1, pp. 1–18, Dec. 2023, doi: 10.1186/S12909-023-04132-4/FIGURES/5.

[18] N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, "Health Records Database and Inherent Security Concerns: A Review of the Literature," Cureus, Oct. 2022, doi: 10.7759/CUREUS.30168.

[19] M. K. Kim, C. Rouphael, J. McMichael, N. Welch, and S. Dasarathy, "Challenges in and Opportunities for Electronic Health Record-Based Data Analysis and Interpretation," Gut Liver, vol. 18, no. 2, p. 201, Mar. 2024, doi: 10.5009/GNL230272.

[20] T. Tsegaye and S. Flowerday, "A System Architecture For Ensuring Interoperability In A South African National Electronic Health Record System," South African Computer Journal, vol. 33, no. 1, pp. 79–110, Jul. 2021, doi: 10.18489/SACJ.V33I1.838.

[21] N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, "Health Records Database and Inherent Security Concerns: A Review of the Literature," Cureus, vol. 14, no. 10, Oct. 2022, doi: 10.7759/CUREUS.30168.

[22] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," PLoS One, vol. 15, no. 12 December, Dec. 2020, doi: 10.1371/JOURNAL.PONE.0243043.

[23] W. Bani Issa *et al.*, "Privacy, confidentiality, security and patient safety concerns about electronic health records," Int Nurs Rev, vol. 67, no. 2, pp. 218–230, Jun. 2020, doi: 10.1111/INR.12585.

[24] K. A. Alarfaj and M. M. H. Rahman, "The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix," Applied Sciences 2024, Vol. 14, Page 5785, vol. 14, no. 13, p. 5785, Jul. 2024, doi: 10.3390/APP14135785.

[25] B. Berisha, E. Mëziu, and I. Shabani, "Big data analytics in Cloud computing: an overview," Journal of Cloud Computing, vol. 11, no. 1, pp. 1–10, Dec. 2022, doi: 10.1186/S13677-022-00301-W/FIGURES/11.

[26] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "PRMS: Design and Development of Patients' E-Healthcare Records Management System

for Privacy Preservation in Third Party Cloud Platforms," IEEE Access, vol. 10, pp. 85777–85791, 2022, doi: 10.1109/ACCESS.2022.3198094.

[27] S. Shafqat, S. Kishwer, R. U. Rasool, J. Qadir, T. Amjad, and H. F. Ahmad, "Big data analytics enhanced healthcare systems: a review," Journal of Supercomputing, vol. 76, no. 3, pp. 1754–1799, Mar. 2020, doi: 10.1007/S11227-017-2222-4/TABLES/7.

[28] S. Haneuse, D. Arterburn, and M. J. Daniels, "Assessing Missing Data Assumptions in EHR-Based Studies: A Complex and Underappreciated Task," JAMA Netw Open, vol. 4, no. 2, Feb. 2021, doi: 10.1001/JAMANETWORKOPEN.2021.0184.

[29] Z. F. Khan and S. R. Alotaibi, "Applications of Artificial Intelligence and Big Data Analytics in m-Health: A Healthcare System Perspective," J Healthc Eng, vol. 2020, no. 1, p. 8894694, Jan. 2020, doi: 10.1155/2020/8894694.

[30] G. S. Nadella, S. Satish, K. Meduri, and S. S. Meduri, "A Systematic Literature Review of Advancements, Challenges and Future Directions of AI And ML in Healthcare," International Journal of Machine Learning for Sustainable Development, vol. 5, no. 3, pp. 115–130, Sep. 2023, Accessed: Sep. 20, 2024. [Online]. Available: https://www.ijsdcs.com/index.php/IJMLSD/article/view/519

[31] M. Mirshafiei, H. Rashedi, F. Yazdian, A. Rahdar, and F. Baino, "Advancements in tissue and organ 3D bioprinting: Current techniques, applications, and future perspectives," Mater Des, vol. 240, p. 112853, Apr. 2024, doi: 10.1016/J.MATDES.2024.112853.

[32] D. A. Matlebjane, "Adoption of blockchain to enhance patients' health information management," 2022. Accessed: Oct. 23, 2024. [Online]. Available: https://ujcontent.uj.ac.za/esploro/outputs/graduate/Adoption-of-blockchain-to-enhance-patients/9915108407691.

[33] National Department of Health "National Digital Health Strategy for South Africa 2019-2024" 2019. Accessed: May 13, 2025. [Online]. Available: https://www.health.gov.za/wp-content/uploads/2020/11/national-digital-strategy-for-south-africa-2019-2024-b.pdf