African Journal of Inter/Multidisciplinary Studies 2025 | *7(1): 1-9* | *DOI:* https://doi.org/10.51415/ajims.v7i1.1509

RESEARCH ARTICLE:

Considering Ethical Issues Affecting Patients' Records Stored on the Cloud in South Africa

Ngoako Marutha[1] and Azwihangwisi Mavhandu-Mudzusi[2]

Received: 18 June 2024 | **Revised:** 19 May 2025 | **Published:** 10 June 2025

Reviewing Editor: Dr. Francis Akpa-Inyang, Durban University of Technology

Abstract

The study sought to investigate the ethical implications of patients' medical and health records being stored on the cloud in South Africa. A literature review was conducted in this qualitative study to examine ethical implications of patients' medical and health records being stored on the cloud in South Africa. It was found that healthcare facilities use private cloud storage, hosted by a third party, across national borders without consideration of any ethical matters. In most instances, healthcare facilities do not request consent from patients before their records are transferred to the cloud in the hands of a third party. A framework is proposed for consideration of ethical issues regarding patients' records that may be stored on the cloud in South Africa. It is envisaged that the framework would minimise violation of ethics principles while avoiding possible litigations to health service providers or information getting misused in the hands of the third party. There are a number of ethical issues surrounding patients' information or records produced during healthcare services rendered to patients and kept in healthcare facilities which need to be considered before seeking service for information keeping from any third party. For different reasons, including insufficient filing space and difficulty in retrieving patients' records during healthcare services, most healthcare facilities apply the latest technologies such as cloud computing to which the decision eventually affect patients' personal information. Patients' information kept on the cloud contain personal information that may eventually affect patients' personal life. One of the issues to be addressed by the study is obtaining patient consent before disclosing their personal information to a third party.

Keywords*: ethical issues; patients' records; record storage; cloud computing; South Africa*

Introduction

The study provides guidance about consideration of ethical issues regarding patients' records stored in the cloud. It is hoped that it will provide significant information through literature review, discussion and recommendations about what organisations in the industry should consider when it comes to putting patients' records in cloud storage. This study will enable the industry to know what to do to ensure the security of their records and patients' information while in the cloud. The study also provides organisations with information about measures to put in place to control access to records in the cloud or even to hold cloud owners accountable for any recorded information containing patients' health and medical history that goes missing or is lost. It will enable them to understand the ethical issues to be considered when they decide on cloud solutions. Many developing countries have started focusing on creating patients' health records in electronic format, known as electronic health records (EHRs). Although EHRs are cost-effective and contribute to high quality in healthcare, consideration of the safety of information created and managed using electronic systems is vital. Electronic systems for managing patients' records may be very useful, but special care must be taken concerning ethical issues of storing the patients' information using these systems (Ozair *et al.*, 2015). For instance, government will need to make provision in policies and procedures for controlling the sharing, receipt and viewing of patients' health information in any format

[1]University of South Africa, emarutns@unisa.ac.za | https://orcid.org/0000-0002-5679-4394
[2]University of South Africa, mmudza@unisa.ac.za | https://orcid.org/0000-0002-6916-8472

DUT DURBAN UNIVERSITY OF TECHNOLOGY INYUVESI YASETHEKWINI YEZOBUCHWEPHESHE
AFRICAN JOURNAL OF INTER/MULTIDISCIPLINARY STUDIES
OPEN ACCESS

or medium. Patients' information will need to be protected at all the times even when healthcare providers interact in serving the patients. Although patients' information is to be disclosed only with the patients consent, other information is allowed for disclosure without consent by other privacy rules (Chiruvella and Guddati, 2021).

Furthermore, with the growth in technology, many organisations started moving from traditional paper-based information management into electronic modus operandi. In so doing newly created information are created electronically into the operational system already in existence, while the old paper-born records are digitised in a form of scanning and capturing into the system to be managed electronically throughout its life. It takes a lot of effort that include funds and labour to successfully move into a digital mode of information management. This will ensure that the organisation follows appropriate procedure in managing such records. In order to properly digitise your records and working system, the organisation will need to identify information targeted for digitisation, prepare such information for the process, making scanning resources and storage available (STARBIC, 2020). This will ensure readiness for the entire process and make sure success is rest assured. As the world continues to move away from 20th century analogue systems of record keeping to postmillennial electronic systems of data capturing, Spriggs, Arnold, Pearce and Fry (2012) emphasise the need for ethical considerations in this regard. Ethical issues of patients' personal information, such as assurance of security and confidentiality, are regularly breached in healthcare facilities with or without intention or knowledge (Marutha and Mosweu, 2021). Ermakova, Fabian and Zarnekow (2014) state that although the phenomenon of cloud computing in healthcare has yet to be researched extensively, this does not mean that ethical issues should not form part of the focal point of these studies. Access Partnership (2020) critically outlines how the growth of artificial intelligence necessitates adequate policies to be in place as far as issues of cybersecurity are concerned. According to Shibambu and Marutha (2021), "*contrary to cloud computing, cloud storage is an offering of cloud computing… It is about storing data with a cloud service provider rather than on local systems such as an external hard drive, a compact disc and many more*".

Cloud computing is used to keep or store EHRs online. Ozair *et al.* (2015) describe EHRs as the various biographical and medical historical records of individual patients, which are stored digitally for safe keeping. Although this simplified form of storing medical records has presented many potential benefits, the easy access medical personnel have to these records has caused considerable debate. This easy access, according to Probha and Prabakaran (2019), has undermined the autonomy of these patients and their consent. Jain and Singh (2017) also identify the main challenges to security in e-healthcare to be trust, legal matters and confidentiality. The Healthcare and Public Health Sector Coordinating Council (HPHSCC) has identified cyberattacks as the greatest threat to health information technology (HPHSCC, 2017). Keeping patients' records on a private cloud may be paramount to ethical breaches since the information transferred to the cloud is kept by a third party. Section 14(1) and (2) of the National Health Act of South Africa deals with confidentiality and stipulates that all information concerning the users, including information relating to their health status, treatment or stay in a health establishment is confidential "unless the user consents to that disclosure in writing; a court order or any law requires that disclosure or non-disclosure of the information represents a serious threat to public health" (Republic of South Africa, 2004). This principle is also stipulated in the Promotion of Access to Information Act 2 of 2000, which states that any third-party person requesting information that is personal should access such information with consent from the person or next of kin of that person in case the person is no longer alive (Republic of South Africa, 2000). The government of South Africa also introduced the Protection of Personal Information Act 4 of 2013 "to promote the protection of personal information processed by public and private bodies…provide for the rights of persons regarding unsolicited electronic communication and automated decision making…regulate the flow of personal information across the borders of the Republic …" amongst other reasons (Republic of South Africa, 2013). This does not exclude patients' personal information about treatments and prescriptions in healthcare facilities.

Although the ICA code of ethics (1996) presents several standards and conduct to guide archivists and records management professionals it still depends on whether the affected countries adopt and legalise such ethics. This is because people are governed by the local legal framework like it is the case with international standards, which need to be adopted by the South African Bureau of Standard (SABS) to South African National Standard (SANS) before they may be applied in the country. Some of the ethical stipulations from the ICA code of ethics (1996) is about protection of records integrity by maintaining originality in the records. It also emphasises abidance to archives and records management principles relating to different activities including maintenance, appraisal, and application of provenance in archival process. Again, this source is more focused on records at the archival level, which is not the focus of this study since patients' personal records are not archival and may be disposed of once the patient dies as part of ephemeral collections.

Methodology

This qualitative study relied on a literature review to formulate a framework for consideration of ethical issues when it comes to keeping patients' records on the cloud, especially a private cloud. The researchers used the Google search engine to find relevant literature from different databases and websites. The keywords used included ethical issues, patients' records, record storage, cloud computing and South Africa, which were extracted from the title of the study. The search engine provided some links with titles and summaries after every search per keyword and the researchers were able to browse through the summaries to check for relevancy before opening the link - the aim of this was to save time. This enabled the researchers to reduce the number of articles to open and scrutinise.

Synopsis of Medical Records Management in South African

Although cloud computing comes with many advantages pertaining to the way records are stored, managed, accessed and disposed of (Shibambu and Marutha, 2021; Marutha, 2016), South Africa, like many other African countries, is still far from applying the latest technologies that includes cloud computing (Marutha, 2023; Marutha, 2016). This result into public healthcare institutions operating in silos as if they are competitors and or serve different clients since they are running of means to share their patients' information (Marutha, 2023; Marutha, 2016). Resistance to the manual mode of operation maintains problems in the management of patients records in the country, and Africa in general, because paper-based records management comes with many disadvantages. These include high turnaround time for retrieval, which eventually affect patients waiting time for healthcare service, which is not the case with electronic records management that may also be kept and shared on the cloud (Marutha, 2023). Besides, in the case of South Africa, any person accessing or using patient medical records must be identifiable. This implies that it must be known who accessed patients' medical history, whether healthcare provider or practitioner. The question is whether this will be possible for records kept on the cloud, especially cloud hosted outside the country by independent and private organisation. Further than this, the healthcare institutions are expected to ensure that healthcare records are kept securely, and that the institution must set up control measures to prevent unauthorised access of any kind. This implies access to whether storage facilities, system or physical records themselves (Health Professional Council of South Africa, 2022; Republic of South Africa, 2004).

Furthermore, any changes or corrections or amendments in the medical records must be dated and signed with visibility of what was changed, and the person making the changes must state the reason for doing it. So, in case of electronic records, it must be clear from the system audit trail what, why, who and why changes were made. This implies that even the cloud computing system must meet all these requirements (Health Professional Council of South Africa, 2022). Health Professional Council of South Africa (2022) shows that as also stipulated in the section 17 (1) of the National Health Act No. 61 of 2003, records of medical nature must be protected against any kind of unauthorised access to prevent information disclosure and protect patients' confidentiality and privacy. Electronic medical data also need to be secured with measures set up as guided by appropriate international standard in any system that might be adopted to keep and manage them. The National Health Act (Act No. 61) of 2003 shows that healthcare providers are not allowed to share patients' healthcare information or records with any third party unless patients give written consent or court issued court order to share the information with specific person or people or company. Patients' medical records are personal and should also be kept confidentially and private in terms of the POPI act of South Africa (Health Professional Council of South Africa, 2022). The question stands, to imagine whether healthcare institutions and practitioners will be able to control records on the cloud bearing these requirements in mind.

Patients' records are required by law to be kept by healthcare facilities when the patients receive the service so that medical practitioners can refer to them when the same patients visit for the same or different healthcare problems in the future. Section 13 of the National Health Act 61 of 2003 of South Africa includes an "obligation to keep records" and it stipulates that "the person in charge of a healthcare establishment must ensure that health records containing such information as may be prescribed is created and maintained at that health establishment for every user of health services" (Republic of South Africa, 2004). Due to the lack of record-keeping space in facilities, most healthcare facilities resort to technologies such as cloud computing. However, there seems to be minimal documentation of ethical issues relating to cloud computing of patients' health records. Ethical issues connected to cloud computing for patients' health records includes but are not limited to patient privacy, information security breaches, records autonomy, host generosity, non-maleficence to patients' data, host fidelity and honesty, total cost, system operational compliance and user-friendliness, data imprecisions, and related information

accountability (Afzal and Arshad, 2021). "The increasing interest of for-profit companies in acquiring the databases of large health care systems poses new challenges to the protection of patients' privacy" (Chiruvella and Guddati, 2021). The other concern is that private hosting entities may have opportunity to exploit millions of patients' data for commercial purposes, especially the vulnerable population of patients in different institutional sphere of influence. When adopting cloud computing host organisation may exploit the information during sharing between patients and healthcare providers, which bring about challenge to be addressed amicably (Chiruvella and Guddati, 2021).

The purpose of the study is to investigate consideration of ethical issues in South Africa regarding patients' records stored in the cloud. The overall objective of the study is to propose a framework for the consideration of ethical issues in South Africa regarding patients' records stored in the cloud.

Ethical Management and Security of Patient Health Records

The findings from literature review encompassed discussions on how ethical considerations of consent, transparency and access to patient records should constantly be adhered to when dealing with digital records. Plausible ways in which electronic records can be used to the benefit of individual patients while upholding the credibility of medical institutions were also examined. Ozair *et al*. (2015) show that EHRs are being implemented extensively in the healthcare fraternity simply because of their many advantages compared to manual paper records. Two major themes emerged from literature appraisal, namely Patient records management and Patient healthcare ethical issues, and cloud computing. Opele and Omole (2019) describe patient records as the official documentation that details an individual's past medical history and that provides guidance for future medical assistance. Patients' records in electronic format, i.e. EHRs, are defined by Ozair *et al.* (2015) as "a record of a patient's medical details (including history, physical examination, investigations and treatment) in digital format". Ferguson (2015) explains how patient health records assist practitioners in guiding individuals on the best medical procedure or advice that needs to be followed. Poor handling of such confidential information has led to many legal battles between individual patients and hospitals (Al-Issa *et al.,* 2019). It is for this reason that hospitals and medical bodies have implemented stringent measures, through comprehensive policies, to ensure that the confidentiality of patient records and the autonomy of the individual's rights to these records are respected (Abbas and Khan, 2015; Gellman, 2009). However, most of these ethical aspects were formulated focusing on records in the form of hard copies, with limited to no focus on cloud computing.

Practitioners, including clinicians and nurses, in healthcare facilities, are expected to strictly comply with ethical principles regarding patients' records, since this information is personal to patients, and to ensure that the information is not disclosed or accessible to third parties without the consent of the patient affected by the information in question (Buttigieg *et al.,* 2015). Ethical issues regarding patients' records include privacy and confidentiality of patients' information, which appears to be a key ethical principle (Ozair *et al*., 2015). Afzal and Arshad (2021) add that "common ethical issues associated with electronic medical records cover patient privacy and security breaches, autonomy, generosity, non-maleficence, fidelity and honesty, total cost, system operation, data imprecisions, and related accountability". Pinto *et al.* (2018) state that the introduction of electronic patient records systems brings more challenges to the healthcare fraternity, including autonomy, since patients' preferences, beliefs and their right to be independent are not considered. The electronic records system at times results in the electronic data jeopardising "autonomy, as a result of some personal information about the patients landing in the wrong hands and that would affect several health and socio-economic matters" (Salerno *et al.,* 2017). Ozair *et al.* (2015) explain that privacy of information is only considered well practised when the patient's information is accessed only with the consent or permission of the patient affected by the information, or their legal guardians or representatives based on their medical condition resulting in their inability to act. There are several security breaches that may pose threats to privacy in patients' medical and health history information (Ozair *et al*., 2015).

The Advent Health University (2020) mentions several considerations of ethical issues regarding patients recorded information. One very important consideration is to think about the best way of obtaining informed consent from patients for sharing or accessing their information. Another is the limitations when it comes to utilisation of records about the patients, especially those that were created, collected and managed electronically using different modem technological devices. Policies and regulations also need to be refocused based on the information management and technology of current times. In using statistical information for health data, institutions must ensure that there

is no room for "de-anonymization of patient data" since that may expose identities of patients (Advent Health University, 2020). Patients should have a certain level of control over their information that is in the possession of health facilities. Appropriate procedures must be applied before the adoption and implementation of new technology and how that will affect patients' lives (Advent Health University, 2020). Although cloud computing itself is not a new phenomenon in the digital age we live in, its use in electronic healthcare is an evolving feature of modern-day medical science (Access Partnership, 2020). The move from physical patient records to electronic data stored on cloud servers has introduced a new aspect to patient records management – artificial intelligence (AI) (Abbas and Khan, 2015). Sivan and Zukarnain (2021) note that although this form of medical technology has helped reduce past inefficiencies of manual record keeping such as inadequate storage and poor record keeping, issues of privacy and cloud security continue to be of great concern. Faragardi (2017) emphasises the need to strengthen security on cloud computing systems in order to ensure that patient records are kept safe. The safety of these records alone is not the only point of focus. Kluge (2016) acknowledges the ethical considerations medical personnel need to practise in keeping and accessing these records. Kluge (2016) further explains how consent needs to be obtained from individual patients when doctors seek to gain access to those records for the purpose of research or referral. Opele and Omole (2015) explain how the electronic storage of patient records has often led medical personnel to undermine basic ethical considerations, such as the right to consent and autonomy of individual patients.

Patient confidentiality and cloud security continue to be the main challenges in electronic healthcare. Sulmasy *et al.* (2017) discuss how patients should have access to their medical records. This would present the kind of transparency which Abbas and Khan (2015) describe as the medical wonders of technological innovation. Sulmas *et al.* (2017) strongly encourage individuals to discuss the records with their practitioners, in order to avoid distortion of information when attempting to understand the content outlined in them. This means that medical personnel should not, at any point, deprive patients of access to their electronic records (Ferguson, 2015). This may be possible with EHRs since they "increase access to health care, improve the quality of care and decrease costs" (Ozair *et al.,* 2015). Probha and Prabakaran (2019) caution that technological advances in electronic healthcare should be consistent and sensitive to ethical considerations. Ozair *et al.* (2015) stress that with EHRs, patients develop a fear that their information may be shared without their consent, and as such they even want their information to be deleted rather than being accessible by a third party. On the other hand, concealing their information may negatively affect their future treatments as clinicians will not have access to understanding their medical and health history before commencing new treatment. Policies and procedures should be reviewed to cover ethical issues regarding the confidentiality and safety of patients' records by responsible accounting officers. Cloud computing has presented many opportunities for growth and modernisation in public health, but possible cyberattacks on servers continue to be the main threat to this platform. Ozair *et al.* (2015) further elaborate that "ethical issues related to EHRs confront health personnel. When patient's health data are shared or linked without the patients' knowledge, autonomy is jeopardized".

Discussion and Proposed Framework

There is no doubt that putting patients' personal information on the cloud hosted by private companies needs patients' consent. This has been affirmed by the Protection of Personal Information Act, the Promotion of Access to Information Act and the National Health Act. All these Acts show that providing access to and/or handing over information to a third party requires informed consent from the person affected by such personal information or the person to whom the information is personal. This implies that failure to obtain informed consent before transferring or handing over the information to the third party is unethical before the law. Healthcare facilities must therefore familiarise themselves with appropriate rules of law because legislative prescripts are mandatory or obligatory rather than a mere suggestion or request. It is highly advisable that healthcare facilities develop or review their operational policies and procedures, especially those dealing with processing patients' information and off-site or cloud computing, so that they adhere to legislative mandates. Keeping business records on the cloud or in off-site storage comes with very serious risks as the handling of such information or even the records in their different media and formats is beyond the owners' control. The reason is that the host organisation or its employees may start using the information in the records for many reasons other than those expected by the owner. Some of the actions may ultimately affect the owner of the information negatively in different ways.

Another issue is that the owner must also know and understand the safety and security measures that are put in place for the cloud storage they are intending to utilise for their patients' records. At times even if the cloud host

may not have intention of using the information for personal gain, their safety and security measures may be threatened if they are not strong enough. Weak safety and security measures that have loopholes may provide an opportunity for hackers and cyberattacks to attack the information stored off-site on the cloud. So, healthcare facilities must have a strategy to ascertain the safety and security of their records before utilising a cloud storage provider. Lastly, facilities must obtain consent from patients or clients since the information contained in the records deals with their health and treatments. Based on the healthcare facility planning, consent may be requested from patients during their consultation, but patients still reserve the right to refuse. It is believed that with clear information and reasons for keeping their records on the cloud, it will be very rare that patients refuse permission. This will also show openness and transparency of the healthcare facilities to their clients. Healthcare facilities may also need to sign a clear lease agreement and/or memorandum of understanding (MOU) covering all issues as required by legislation with the third party that will be hosting the records on the cloud.

Additional to the recommendations of the study, a framework is proposed for the consideration of ethical issues regarding patients' records stored on the cloud (see figure 1 below). Overall, the framework recommends that healthcare facilities consider legislation as a foundation for the governance of patients' information and knowledge. There are many pieces of legislation that may be applied but the most fundamental Acts are the National Health Act, the Protection of Personal Information Act and the Promotion of Access to Information Act. These three Acts directly address matters pertaining to personal information, processing and access.

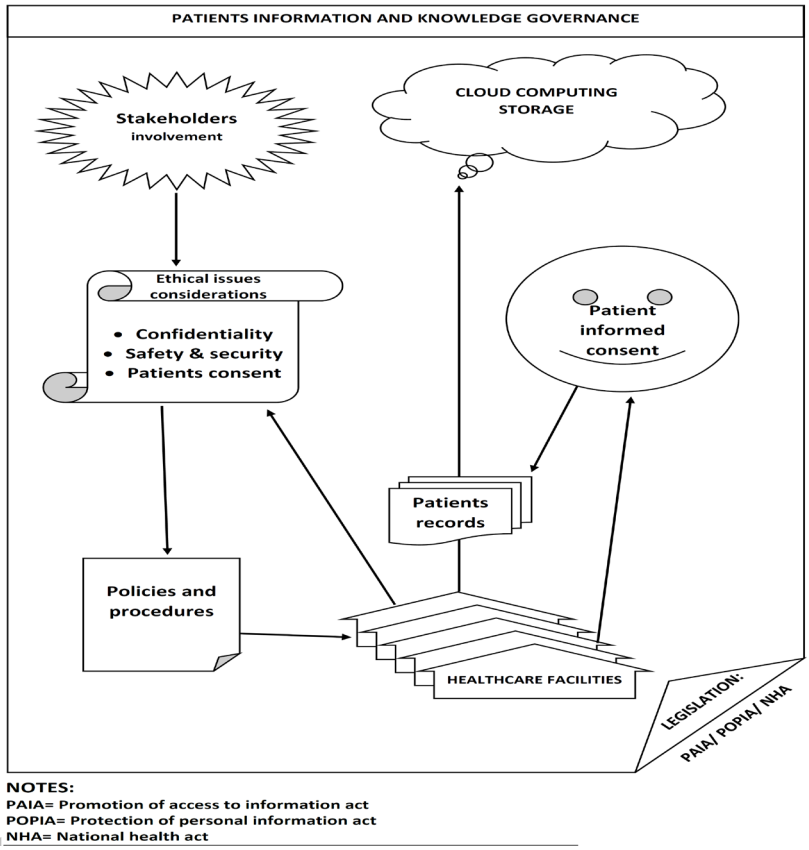

Figure 1: Framework for consideration of ethical issues regarding patients' records stored on the cloud

The framework shows that healthcare facilities should consider and analyse ethical issues before they even decide to transfer patients' personal information to cloud computing. Confidentiality, patient consent, safety and security should be amongst the issues to be prioritised. The healthcare facilities should then consider developing their own policies, procedures and other guidelines to support delegated staff members in doing the right things the right way when it comes to keeping patients' records on the cloud. It is vital that when healthcare facilities start keeping their patients' records on the cloud, patients be invited to give written, informed consent. Healthcare facilities should make sure that ethical issues are covered in both local policies and procedures as well as in the lease agreement or MOU signed with the cloud storage host organisation, which must also cover issues of safety and security. Accounting officers of the healthcare facilities must ascertain that the healthcare facility follows appropriate

procedures as set out in different guidelines before implementation is authorised. Stakeholders such as SITA, NARS and national health and records management professional bodies may also need to be consulted for different expertise. Generally, healthcare facilities must assess whether the cloud host meets all ethical requirements, especially those affecting patients directly.

The study may be used as a resource for policy makers in the healthcare industry to ensure that patients' records stored in the cloud are secure. Policies should be reviewed to cover appropriate procedures, leading to a secured form of cloud computing of patients' records. Organisations in the healthcare fraternity may have their own best practice for secured record keeping of patients' health and medical history which is readily available only to authorised people as required by the legislative framework governing patient healthcare and records management. Finally, the healthcare fraternity may find a way to ensure the confidentiality and security of their patients' information kept in the cloud. Patients will remain secured from any third party that has the intention to use their information negatively.

Conclusion

In conclusion, it is a legislative requirement that patients give an authorising party consent for their own personal information to be shared or to be given to a third party. Patients have the right to take legal action against the service provider sharing their personal information with a third party without their consent. This implies that healthcare facilities take a very high risk of giving patients' personal information to a third-party without their consent. It is usually very easy for the healthcare facilities to request consent from the patients during service delivery and the records creation moment. This may be done by frontline staff explaining to patients and letting them sign to agree or disagree. Cloud computing has many advantages, including cost reduction and quick access to information, but proper procedures need to be followed in adopting this technology. The only major disadvantage is that the records are beyond the facility's control, but this problem may be resolved by signing lease agreements and an MOU as a binding legal commitment between the two parties.

Declarations

Interdisciplinary Scope: The article demonstrates an interdisciplinary scope by integrating insights from organisational communication, language studies, organisational behaviour, and education.

Author Contributions: All authors contributed equally to writing all sections of the article; however, the article is based on the first author's master's thesis. The authors declare this article is their original work and all the materials used are appropriately acknowledged and explicitly referenced.

Conflict of Interest: The authors declare no conflict of interest.

Funding: The authors received no financial support for the publication.

Availability of Data: N/A

References

Abbas, A. and Khan, S. U. 2015. e-Health Cloud: Privacy Concerns and Mitigation Strategies. In: Gkloulalas-Divanis, A. and Loukides, G. eds. *Media Data Privacy Handbook*. New York: Springer, 389-421.

Access Partnership. 2020. Artificial Intelligence for Africa: An Opportunity for Growth, Development and Democratisation. Available: https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf (Accessed 02 August 2021).

Advent Health University. 2020. 6 Ethical Issues in Healthcare in 2020. Available: https://online.ahu.edu/blog/ethical-issues-in-healthcare/ (Accessed 16 April 2022).

Afzal, S. and Arshad, A. 2021. Ethical Issues among Healthcare Workers Using Electronic Medical Records: A Systematic Review. *Computer Methods and Programs in Biomedicine Update,* 1: 100030.

Al-Issa, Y., Ottom, M. A. and Tamrawi, A. 2019. eHealth Cloud Security Challenges: A Survey. *Journal of Healthcare Engineering,* 19: 1-15.

Buttigieg, S. C., Rathert, C., D'Aunno, T. A. and Savage, G. T. 2015. International Research in Health Care Management: Its Need in the 21st Century, Methodological Challenges, Ethical Issues, Pitfalls, and Practicalities. *Advances in Health Care Management*, 17: 3-22.

Chiruvella, V. and Guddati, A. K. 2021. Ethical Issues in Patient Data Ownership. *Interactive Journal of Medical Research*, 10(2): e22269.

Ermakova, T., Fabian, B. and Zarnekow, R. 2014. Acceptance of Health Clouds: A Privacy Calculus Perspective. *Proceedings of the European Conference on Information Systems (ECIS),* 1-13.

Faragardi, H. R. 2017. Ethical Considerations on Cloud Computing Systems. *Proceedings*, 1(3): 166.

Ferguson, A. 2015. Introduction to Records Management. *Shropshire Community Health,* 2(5): 1-15.

Gellman, R. 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Available: www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf (Accessed 2 August 2021).

Health Professional Council of South Africa (HPCSA). 2022. Guidelines on Patient Recordkeeping. Available: Link (Accessed 21 March 2024).

HPHSCC. 2017. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf (Accessed 02 August 2021).

ICA. 1996. Code of Ethics. Available: https://www.ica.org/sites/default/files/ICA_1996-09-06_code%20of%20ethics_EN.pdf (Accessed 02 August 2021).

Jain, J. and Singh, A. 2017. A Survey on Security Challenges of Healthcare Analysis Over Cloud. *International Journal of Engineering Research and Technology,* 6(4): 905-912.

Kluge, E. W. 2016. Ethics for Health Informatics Professionals. Available: https://imia-medinfo.org/wp/wp-content/uploads/2015/07/Handbook-for-revised-Code-of-Ethics.pdf (Accessed 02 August 2021).

Marutha, N. S. 2016. A Framework to Embed Medical Records Management into the Healthcare Service Delivery in Limpopo Province of South Africa. University of South Africa, doctoral thesis.

Marutha, N. S. 2023. The Application of Cloud-Computing Technology to Improve Patients' Medical History Access to Clinicians for Quality of Care in the Fourth Industrial Revolution. In: El-Baz, A. and Suri, J. S. eds. *Cloud Computing in Medical Imaging*. New York: Taylor & Francis Group, 111-124.

Marutha, N.S. and Mosweu, O., 2021. Confidentiality and Security of Information in the Public Health-Care Facilities to Curb HIV/AIDS Trauma among Patients in Africa. *Global Knowledge, Memory and Communication,* 70(8/9): 684-696.

Opele, J. K. and Omole, S. M. 2019. The Management of Health Records Libraries through the Lens of Ranganathan's Theory. *Library Philosophy and Practice,* 12(7): 1-15.

Ozair, F. F., Jashmed, N., Sharma, A. and Aggarwal, P. 2015. Ethical Issues in Electronic Health Records: A General Review. *Perspective in Clinical Research*, 6(2): 73-76.

Pinto, S., Caldeira, S., Marques, G. and Da Conceição, A. 2018. Healthcare Technologies: An Ethical Discussion. *British Journal of HealthCare Management,* 24(2): 65–70.

Probha, J. R. and Prabakaran, S. 2019. Security in Cloud Healthcare. *International Journal of Recent Technology.* 8(4): 6164-6171.

Republic of South Africa. 2000. Promotion of Access to Information Act No. 2 of 2000. Available: https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf (Accessed 23 September 2021]).

Republic of South Africa. 2004. National Health Act, No. 61 of 2003. Available: https://www.gov.za/sites/default/files/gcis_document/201409/a61-03.pdf (Accessed 23 September 2021).

Republic of South Africa. 2013. Protection of Personal Information Act, No. 4 of 2013. Available: Link (Accessed 23 September 2021).

Salerno, J., Knoppers, B., Lee, L., Hlaing, W. and Goodman, K. 2017. Ethics, Big Data and Computing in Epidemiology and Public Health. *Annals of Epidemiology,* 27(5): 297–301.

Shibambu, A. and Marutha, N. S. 2021. A Framework for Management of Digital Records on the Cloud in the Public Sector of South Africa. *Information Discovery and Delivery,* 50(2): 165-175.

Sivan, R. and Zukarnain, Z. A. 2021. Security and Privacy in Cloud-Based E-Health System. *Summetry*, 13(5): 742.

Spriggs, M., Arnold, M. V., Pearce, C. M. and Fry, C. 2012. Ethical Questions must be Considered for Electronic Health Records. *Journal of Medical Ethics,* 38(9): 535–539.

STARBIC. 2020. Steps Involved in Digitization of Records and How it Benefits Organizations? Available: https://starbic.com/steps-involved-in-digitization-of-records-and-how-it-benefits-organizations/ (Accessed 21 January 2023).

Sulmasy, L. S., Lopez, A. M. and Horwitch, C. A. 2017. Ethical Implications of the Electronic Health Record: In the Service of the Patient. *Journal of General Internal Medicine*. 32: 935-939.