International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:14, No:11, 2020

Data Integrity: Challenges in Health Information Systems in South Africa

T. Thulare, M. Herselman, A. Botha

***Abstract*—**Poor system use, including inappropriate design of health information systems, causes difficulties in communication with patients and increased time spent by healthcare professionals in recording the necessary health information for medical records. System features like pop-up reminders, complex menus, and poor user interfaces can make medical records far more time consuming than paper cards as well as affect decision-making processes. Although errors associated with health information and their real and likely effect on the quality of care and patient safety have been documented for many years, more research is needed to measure the occurrence of these errors and determine the causes to implement solutions. Therefore, the purpose of this paper is to identify data integrity challenges in hospital information systems through a scoping review and based on the results provide recommendations on how to manage these. Only 34 papers were found to be most suitable out of 297 publications initially identified in the field. The results indicated that human and computerized systems are the most common challenges associated with data integrity and factors such as policy, environment, health workforce, and lack of awareness attribute to these challenges but if measures are taken the data integrity challenges can be managed.

***Keywords*—**Data integrity, data integrity challenges, hospital information systems, South Africa.

I. Introduction

SOUTH Africa is known for its progressive constitution with strong protection of human rights and the right of all its citizens to access high-quality health care but challenges in providing high-quality health care remain [1]. Challenges facing the healthcare system in South Africa are, according to [2], unequal distribution of resources, management, and leadership crisis, increased disease burden, pull and push factors and slow progress in restructuring the healthcare system, including strategies adopted by the government to improve the quality of healthcare delivery.

Hospital information systems (HIS) are increasingly becoming a healthcare tool for the efficient delivery of high-quality health services, as these systems can integrate patient information and change the communication patterns between different hospital wards and healthcare professionals [3]. However, in an information system that contains sensitive and confidential data, there is a need to put certain measures in place to ensure the integrity of data. If not mitigated in time, this can negatively affect the quality of services as indicated by [4] due to authorized users who can make alterations such as modification, deletion, or corruption of data.

In South Africa, the eHealth strategy states that patient-based information systems must be implemented in all facilities where healthcare is provided and that all indicator data should be derived from data that were electronically collected at the place of care [1]. There is evidence of health information systems in some areas in South Africa, but more than half of South Africa's public health centers still use a paper-based filing system [5]. The health information systems are fragmented with no integrated electronic health records [6].

A paper-based system is a traditional approach to maintaining patient health information. The medical records are then stored in a closed room under lock and key [7]. This form of record-keeping has contributed to long waiting times for patient as well as file loss and duplication, lack of resources in medicine and equipment, poor hygiene and poor infection control measures and the overall provision of quality healthcare in South Africa [2], [1], [8].

With the current Covid-19 pandemic, the paper-based system has raised some concerns about the data reporting mechanisms in the country. Dr. Angelique Coetzee, the chairperson of the South African Medical Association (SAMA) states, “The provinces are still on a paper system. We are in the fourth industrial revolution, but our healthcare system is still in the first industrial revolution” [9].

The issue of data integrity is one of the most challenging concerns in the healthcare industry around the world [10]. According to [11], the British Medicines and Healthcare products Regulatory Agency (MHRA) issued guidelines on data integrity in response to concerns that insiders could change data in clinical trials and put patients at risk.

Data integrity is the process of maintaining data and ensuring accuracy and consistency throughout its life cycle [12], [13]. Data integrity in health information systems affects manual and automated decision-making processes, and data integrity issues affect the reuse of medical data for quality improvement, public health, and research [14] as well as impose intangible social costs and undermine public trust in the Government [15].

Data integrity is equally important for both paper (manual) and electronic data as eluded by [16] and should not only be ensured on a technical but also on a human level. It is always better to take proactive action against data integrity issues, rather than taking action as a part of compliance [16]. This means that the levels of authentication, access control, and decision-making must be defined and implemented at an early stage to ensure the integrity of the data of such systems at different stages and improve the quality and effectiveness of healthcare services [17], [18].

Tumiso Thulare is with UNISA, South Africa (e-mail: TThulare@csir.co.za).

The research question for this paper is: What are the data integrity challenges faced in HIS? In this paper, we identify the challenges associated with data integrity. These challenges were found to affect the quality of healthcare services of health information systems in South Africa.

The remainder of the paper is laid out as follows. Section II is the methodology, followed by Section III, literature review. Section IV will discuss and analyze the results and Section V will conclude the research.

II. Methodology

A scoping review is a common approach that is applied to review health research evidence and is suitable for addressing exploratory research questions [19] as opposed to a systematic literature review that focuses on providing answers to a limited question [20]. Relevant sources were identified from the following online databases: IEEE Xplore, Scopus, CSIR Library, ProQuest, National Center for Biotechnology Information, Harzings Publish, Google and Google Scholar dated from 2011 to 2020.

The search identified 34 articles out of 1366 articles, which included search terms: 'data integrity' and health; "data integrity issues"; "hospital information systems" and "challenges". The inclusion and exclusion criteria as illustrated in Table I was applied in the screening process to acquire the chosen articles.

TABLE I
Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
Articles are written in English	Non-English articles
Newspapers, Government documents, gazettes	Abstracts were excluded
Articles including or discussing data integrity, data integrity issues	Articles examining security-based concerns
Articles that are relevant to the topic and question	Articles not relevant to the research question
Articles that are relevant in the domain	Articles not relevant to the domain

As a result of the screening process, 297 full-text articles were identified. Full-text records were read and 263 records that included abstracts and duplicates were excluded. At the end of the screening process, 34 records were selected by utilizing the inclusion and exclusion criteria. Fig. 1 illustrates a flow diagram of the identification, screening, and eligibility searching and filtering process.

III. Literature Review

Data integrity issues pose a high risk and are not always easily detectable. Data integrity-related issues have been uncovered around the world, and are expected to increase in the future [21]. According to [22], the chance of a breach involving 100,000 records in the next two years is 1.2%.

WHO [23] guidelines suggest that data integrity issues may occur based on excessive trust in human practices; the use of computerized systems that are not adequately managed and validated; and lack of adequate review and management of original data and records.

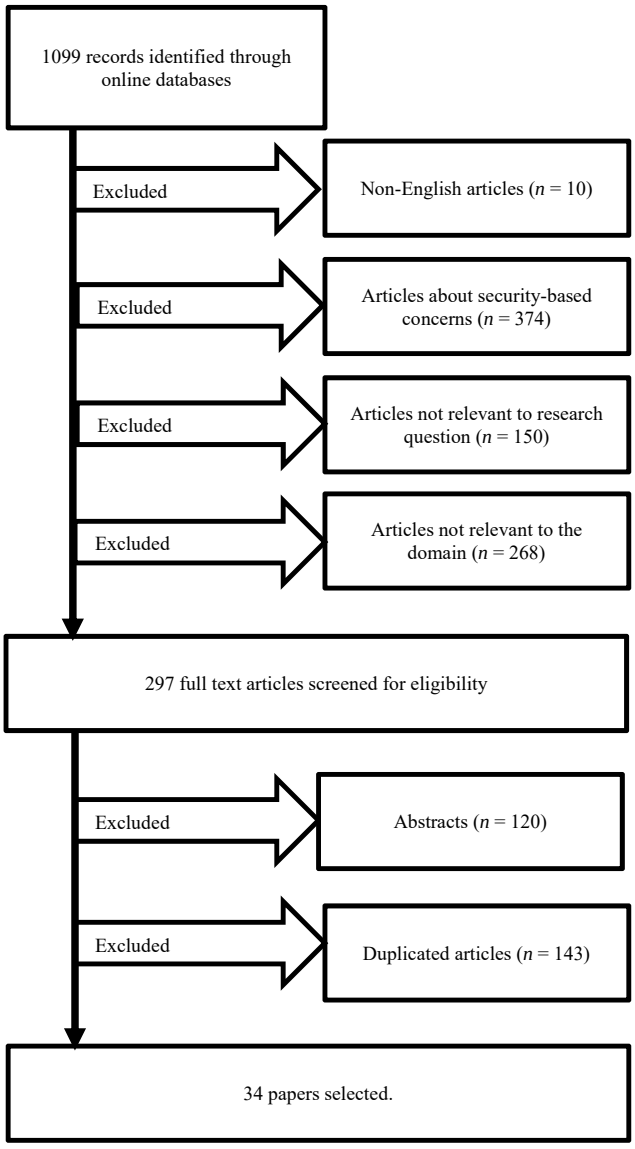

Fig. 1 Flow diagram of the record selection process

According to [24], data integrity errors often result from humans, non-compliant operating procedures, data transmission errors, software errors, compromised hardware, and compromises on physical devices.

IBM's Cost of Data Breach Study in 2019 found that the healthcare industry still has the highest per capita cost of data breaches. The average per capita data breach cost in South Africa was found to be $3.06 million in 2019, an increase of $1.16 million since 2015. Human error and system failures were still the main cause of almost 49% of data breaches examined in the report. South African companies had the highest percentage of organizations that had not used security automation that enabled security technologies to augment or replace human intervention [22].

Masrom and Rahimly [25] state that hospitals face several issues related to storing, sharing, and distributing patient

health records and using hospital methods manually, and human memory. The authors further mention that the most common issues in HIS are human error, hackers, missing or stolen paper, and software errors.

The following section will discuss the challenges associated with HIS and include challenges with human errors, computerized systems, and data integrity.

A. Human Error Challenges

Human errors include both intentional and unintentional issues.

1) Unintentional Human Issues

Unintentional human issues are often the results of poorly developed processes and procedures, mistakes, or lack of understanding [26]. According to [27], this is usually due to inadequate or ineffective employee training, which is usually done haphazardly and should rather be done gradually to provide better knowledge of data integrity.

In South Africa, where data capturers have to enter clinical data from paper, this has resulted in the lack of continuity of care due to missing or duplicate files, which further leads to inaccurate reporting on the numbers, treatment, and results [28], [29].

Bantom [30] highlighted some effects of missing files in South African hospitals. A hospital in the Mpumalanga province could not conclude the previous diagnosis of the patient leading to delays in the delivery of service. Another case in a hospital in Limpopo found that doctors could not operate on a patient because of a missing health record that the doctor needed to make an informed decision based on the medical history of the patient.

2) Intentional Human Issues

Intentional human issues arise from people deliberately disclosing patient information without permission, theft, deliberate modification of data, and deliberate destruction of data [31].

According to [9], the public healthcare system state report revealed that there was a deliberate undercounting particularly with regard to the recorded and reported incident and causes of deaths further questioning the integrity and accuracy of government Covid-19 statistics.

Mahlaola and Van Dyk [32] observed that health information was shared via BBM or Facebook, which was considered intentional. This is because the Internet does not guarantee unauthorized viewing and use of personal information. Therefore, these social platforms are equally vulnerable to internet hacking.

In the Eastern Cape Province, a healthcare professional at a hospital was caught in the act of stealing the patient medical record for litigation purposes by the patient's families [30].

B. Computerized Systems' Challenges

Barrett [33] states that data integrity suffers from common problems with accuracy creating significant impacts. In computerized systems, issues in data integrity management can be due to a poor or complete lack of system controls.

Computer viruses are one of the most common and malicious forms of intentional computer manipulation, that pose a serious threat to computerized patient data as well as healthcare applications [31]. In addition to viruses, trojans, spyware, worms, and ransomware are common malware that have the same effects.

A software error in a HIS contains hundreds or thousands of medical records, i.e. a mistake that results in an inaccurate record of patient allergies or medication can adversely affect a large number of patients. Software errors can mess up data, delete information, or put it in the wrong place [34].

The information value chain begins with clinical users interacting with information from IT systems before considering decisions and taking action [35]. This makes them all too aware of the difficult relationship they have with information systems [36]. Often these information systems are so complex that users cannot analyze or understand the computations and therefore cannot carry out daily activities [34].

A study [37] found that the graphical user interface (GUI) of the information system showed different information such as patient notes, blood investigation, and medication on different windows. This allows users to open only a limited number of windows concurrently. As a result, users have to memorize, write down, or copy and paste the necessary information before switching to another window. This tedious procedure is prone to result in delays and mistakes.

Information systems features such as "cut and paste" or drop-down menus have contributed to poor data quality. The use of this feature by health professionals can lead to inaccuracies or authorship integrity issues that may lead to health risks and labilities since documentation cannot be tracked to the source [4], [33].

Coiera and Ash [36] and Amato and Salazar [38] found that issues in Clinic Decision Support Systems (CDSSs) and Computerized Physician Order Entry (CPOE) included duplication of orders and selection orders where the user might pick the wrong drug, dose frequency or formulation from a drop-down menu.

The risks of copy/paste include inaccurate, or outdated information; redundant information, which causes the inability to identify the current information; inability to identify the author or intent of documentation; inability to verify when the documentation was first created; propagation of false information; internally inconsistent progress notes and billions lost to billing errors [34], [39].

OIG [40] states that unsecured networks compromise the integrity of health information. Outsiders or employees could have access to the personal data of the systems and beneficiaries. Similarly, [41] mentions that unauthorized users can gain access and falsify data or destroy a system if it is connected to an unsecured network while a hardware malfunction can lead to improper software behavior, which can seriously damage the stored data. For example, read/write head problems in hard drives can leave stale or corrupt data [42].

Health institutions today do not have rigorous, real-time, or

even close-to real-time approach to routinely assess the safety of their health information systems and identify integrity issues [43].

In the next section, we explore factors that attribute to data integrity challenges.

C. Factors Attributing to Data Integrity Challenges

Factors emanating from policy, the environment, health workers, and the lack of awareness were found.

1) Policy

The underlying causes for human error as a precursor to breaches, as mentioned by [32], are inadequate knowledge of security policy, a stressful environment concerning time pressures, and limitations in the system design. Some data integrity issues may be intentional due to the deliberate intent to ignore data security policies.

The South African Professionals Council for South Africa [44] states that no information is removed from or included in the medical record. In addition to protecting medical records, no one is allowed to falsify, add, delete, or modify information from a medical record [45]. The Protection of Personal Information Act 4 of 2013 consists of eight conditions, one of which is security safeguards, which compels institutions to take measures to ensure the confidentiality and integrity of the information [46].

Anthony [47] states that medical record corrections should be made by drawing a single black line to clear the error and add the change and the reason(s) to ensure the originality and authenticity of the medical records.

Most rural healthcare institutions have limited or non-existent access to electronic patient healthcare records [30].

The study [32] found that the uncovered integrity issues were committed by participants who were poorly informed about their organization's policy on electronic data security. Luthuli and Kalusopa [48] reveal the lack of medical records management policy, procedure, and tools that impacted service delivery in public hospitals.

In the case where information systems existed, [49] found that data in the system was corrupt due to the lack of compliance with the data handling procedures.

2) Environment

The physical environment of a workplace can make a significant contribution to the number of errors that occur. According to [2], most facilities in South Africa suffer from poor waste management, lack of cleanliness, and poor maintenance of grounds and equipment. This can contribute to poor working conditions in public hospitals due to psychological stress, job dissatisfaction, burnout, shortage of material resources, equipment, and supplies, and infrastructure [52], [6].

Patients are turned away or left unattended for longer than necessary in public hospitals due to situations such as long queues, inadequate numbers of personnel, lack of admission beds, lack of water, and electricity failures which lead to the cancellation of surgeries [51].

Culture also plays an important role in solving environmental problems. Often, end users know the right course of action, but cannot follow it, because there is an easier way to do something, or they just do not think it is important. An organizational culture where data integrity is not always relegated to the background can result in fewer general mistakes [37], [50].

3) Health Workforce

The serious lack of human resources has led nurses to perform tasks that they are not competent, licensed, or registered to perform. This has led to unqualified nurses who have to perform duties that are supposed to be done by professional nurses and this inadequacy can threaten the health and safety of the patient [53], wherein other cases professional nurses are forced to perform sub-category duties leaving the professional duties unattended to [51].

Barron and Padarath [54] attribute the lack of human resources to the unequal distribution of health professionals between the private and public sectors. They indicate that these can be combined with the unequal distribution of health professionals in the public sector between provinces. Also, the patient influx and quadruple burden of diseases on the South African health system are other challenges to consider [2].

Human resources challenges for health in South Africa as seen from Fig. 2 at the time of the study were associated with: inadequate funded posts; misdistribution of posts relative to need; poor service delivery planning; overworked clinicians; safety concerns for staff in facilities; lack of financial resources to absorb junior doctors in the public health sector, to name a few [6]. These challenges have forced many professional nurses to leave the country in search of better pay and working conditions abroad such as the United Kingdom, Australia, New Zealand, Canada, and the United Arab Emirates [55].

4) Lack of Awareness

Many human errors are from end-users simply not knowing what the right course of action is in the first place [50]. Human awareness in healthcare organizations is the primary need because it is the users who will be facilitated by secure technologies and approaches in a healthcare organization [10].

According to [56], the lack of awareness is an obstacle to reliable data and information. It is one of the key factors that hinder the delivery of high-quality services in healthcare facilities in South Africa [57], [7], [48], [6], [58], [2].

IV. Results

The findings from the literature reveal that the challenges faced in health information systems, particularly in HIS include, human errors that may be intentional or unintentional and those emanating from computerized systems. The research then further explored the factors that attribute to the identified challenges in HIS that cause data integrity issues. These factors include policy, environment, health workforce, and lack of awareness.

Fig. 2 Challenges Facing Human Resources for Health, adapted from [6]

The following section will give recommendations to the factors that contribute to data integrity issues and if applied can assist to manage data integrity challenges.

A. Policy

It should be noted right from the start that data integrity and data security are not the same and that everyone in an organization must adhere to a data security policy.

While the Protection of Personal Information Act (POPI) [59], the set standards and guidelines of the Health Professional Council of South Africa (HPCSA) [60] and the District Health Information Software (DHIS) [61] are implemented at healthcare institutions on how health information is created, used, transmitted, stored, retrieved, controlled and preserved, there is a need for the implementation of a data integrity policy.

The best way to communicate data integrity practices is to develop a data integrity policy that everyone should follow. A written data integrity policy should be implemented for both the paper-based and computer-based systems that clearly define what constitutes raw data, source data metadata and a "complete data set" [23] and define how one is supposed to handle the information, as well as how the validation process happens [62].

Holistically a data governance framework that comprises policies and regulations, data strategy and leadership, data ecosystems, and invested data technologies can mitigate risks to government and society from poor data quality, data falsification, data obsolescence, and security threats [15].

B. Environment

Organizational culture has the potential to increase the likelihood of intentional or unintentional errors in data integrity. To reduce this potential, companies should strive for an open culture in which subordinates can question the hierarchy, and full reporting of a systemic or individual error is a business expectation [63].

The National Department of Health should give priority to the provision of adequate and appropriate resources. Securing funding for hospital infrastructure to revitalize clinics and hospitals should also be regarded as a high priority.

C. Health Workforce

Health workers and trainees are assaulted on duty and therefore it is necessary to ensure physical safety on the way to and from work. Currently, employees have negative morale. Human resource planning that includes long-term transition and succession planning for sustainability will be required [6].

The Government needs to improve security in healthcare facilities by introducing the necessary security measures to protect health professionals. In-service training may be needed to update and inform professional nurses about the roles and responsibilities of the unqualified workers. These workers' skills should be developed and they should be supervised to ensure that they provide an adequate level of service to patients. The ultimate goal in addressing the shortage of the health workforce is for the government to review training programs that capacitate the human workforce to meet the healthcare needs of the population.

To retain professional nurses, it is recommended that budgetary allocations are increased which include financial or non-financial incentives for nurses, recruitment strategies, and the correct job distributions.

D. Lack of Awareness

Health professionals at all levels must understand the importance of data integrity and the impact that they can have on the integrity of health information, thus enabling them to make better decisions or seek help if they are not sure about the repercussions of a particular action. Training has been widely emphasized in many studies and it is an essential part of raising awareness. The training should not be a once-off but should be carried out periodically. Training must be relevant and engaging. The use of interactive training courses that use image and video content is better than hour-long power-point sessions, especially in the current COVID-19 pandemic scenario [50].

V. Conclusion

Despite the political commitment and strong policies for the protection of health information, South African hospitals still lack sound policies and regulations about data integrity. The absence of these policies and guidelines has been noted due to the lack of the provision of quality healthcare services.

Data integrity challenges in HIS have been identified in human and computerized systems. The research further explored the factors contributing to these challenges and found that these were related to policy, environment, health workforce, and lack of awareness. Creating and maintaining a work environment and organizational culture that support data integrity can help minimize data integrity challenges.

Hospital data security policies must be reviewed to develop

and implement data integrity policies for HIS to provide accurate, complete, and timeless health information. The South African health information system employees should be aware of the importance of data integrity and the problems associated with inaccurate health information.

The researcher hopes that this document will highlight the importance and impact of data integrity challenges should they not be managed.

REFERENCES

[1] NDOH, "National Digital Health Strategy for South Africa 2019 - 2024", in *Better health for all South Africans enabled by person-centered Digital Health*. 2019, Department of National Health: South Africa.

[2] W. T. Maphumulo and B. R. Bhengu, "Challenges of quality improvement in the healthcare of South Africa post-apartheid: A critical review". *Curationis*, 42(1): p. 1-9, 2019.

[3] F. M. Najem, "The Impact of Hospital Information System Quality on the Health Care Quality: A Case Study on European Gaza Hospital", in *Department of Business Administration*. 2016, The Islamic University-Gaza. p. 190.

[4] P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, and F. Whittaker. "Ensuring data integrity in electronic health records: a quality health care implication". in *2016 International Conference on Orange Technologies (ICOT)*. IEEE, 2016. 20-27.

[5] M. C. Katurura and L. Cilliers, "Electronic health record system in the public health care sector of South Africa: A systematic literature review". *African journal of primary health care & family medicine*, 10(1): p. 1-8, 2018.

[6] O. Shisana, "Presidential Health Summit 2018", in *Strengthening the South African health system towards an integrated and unified health system*. 2018, Department of Health: Johannesburg.

[7] P. Mathebeni-Bokwe, "Management of medical records for healthcare service delivery at the Victoria Public Hospital in the Eastern Cape Province: South Africa", in *Department of Library and Information Science*. 2015, University of Fort Hare.

[8] B. Malakoane, J. C. Heunis, P. Chikobvu, N. G. Kigozi, and W. H. Kruger, "Public health system challenges in the Free State, South Africa: a situation appraisal to inform health system strengthening". *BMC Health Services Research*, 20(1): p. 58, 2020.

[9] A. Karrim. "Covid-19 data: SA still in 'first industrial revolution', reporting infections via old 'paper system'". 2020 02 August 2020]; Available from: https://www.news24.com/news24/SouthAfrica/News/covid-19-data-sa-still-in-first-industrial-revolution-reporting-infections-via-old-paper-system-20200802-2?isapp=true.

[10] A. Pandey, A. Khan, Y. Abushark, M. M. Alam, A. Agrawal, R. Kumar, and P. R. Khan, "Key Issues in Healthcare Data Integrity: Analysis and Recommendations". *IEEE Access*, 8: p. 40612-40628, 2020.

[11] J. Pollard, J. Blankenship, and T. Lyness, "Beware The Coming Data Integrity Crisis", in *Data Tampering Will Threaten Your Digital Transformation*. 2018.

[12] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu. "Blockchain Based Data Integrity Service Framework for IoT Data". in *2017 IEEE International Conference on Web Services (ICWS)*. 2017. 468-475.

[13] S. Pearlman. "What is Data Integrity and Why Is It Important?". What data integrity isn't 2019 8 August 2019 [cited 2019 20 September]; Available from: https://www.talend.com/resources/what-is-data-integrity/.

[14] P. Ranade-Kharkar, S. E. Pollock, D. K. Mann, and S. N. Thornton, "Improving Clinical Data Integrity by using Data Adjudication Techniques for Data Received through a Health Information Exchange (HIE)". *AMIA ... Annual Symposium proceedings. AMIA Symposium*, 2014: p. 1894-1901, 2014.

[15] UN, "E-Government Survey 2020", in *Digital Government in the Decade of Action for Sustainable Development*. 2020, Department of Economic and Social Affairs: United Nations, New York.

[16] M. S. Bhadrashette, "Overview of Data Integrity issues in the Pharmaceutical industry". *International Journal of Pharmaceutical Sciences Review and Research*, 14: p. 95-101, 2018.

[17] S. Soares, *Data Governance in a Box: An End-to-End Approach to Operationalize Data Governance*. USA: Information Assets LLC^, 2016.

[18] R. Ganiga, R. M. Pai, M. M. Pai, and R. K. Sinha, "Security Framework for cloud based Electronic Health Record (EHR) system". *International Journal of Electrical and Computer Engineering (IJECE)*, 10(1): p. 455-466, 2020.

[19] H. I. Colquhoun, D. Levac, K. K. O'Brien, S. Straus, A. C. Tricco, L. Perrier, M. Kastner, and D. Moher, "Scoping reviews: time for clarity in definition, methods and reporting". *Journal of Clinical Epidemiology*, 67: p. 1291-1294, 2014.

[20] J. Peterson, P. F. Pearce, L. A. Ferguson, and C. A. Langford, "Understanding scoping reviews: Definition, purposes, and process". *Journal of the American Association of Nurse Practitioners*, 29(2017): p. 12-16, 2016.

[21] A. Agrawal and N. R. Alharbe, "Need and Importance of Healthcare Data Integrity". *International Journal of Engineering and Technology (IJET)*, 11(4): p. 854-859, 2019.

[22] IBM, "The Cost of a Data Breach". 2019, Ponemon Institute.

[23] WHO, "Guideline on Data Integrity". 2019, World Health Organization.

[24] W. Yadow. "3 Key Data Integrity Testing Strategies for DW/ BI Systems". 2019 [cited 2020 3 July 2020]; Available from: https://www.lightsondata.com/3-key-data-integrity-testing-strategies-for-dw-bi-systems/.

[25] M. Masrom and A. Rahimly, "Overview of Data Security Issues in Hospital Information Systems". *Pacific Asia Journal of the Association for Information Systems*, 7(4): p. 51-66, 2015.

[26] C. Curz, "Data Integrity, Data Analysis and Monitoring". 2018, PDA.

[27] H. Balfour "Exploring data integrity guideline changes moving into 2020". 2020.

[28] G. Wright, D. O'Mahony, and L. Cilliers, "Electronic health information systems for public health care in South Africa: a review of current operational systems". *Journal of Health Informatics in Africa*, **4**(1), 2017.

[29] T. E. Mutshatshi, T. M. Mothiba, P. M. Mamogobo, and M. O. Mbombi, "Record-keeping: Challenges experienced by nurses in selected public hospitals". *Curationis*, 41(1): p. e1-e6, 2018.

[30] S. A. Bantom, "Accessibility to Patients' own Health Information: A Case in Rural Eastern Cape, South Africa", in *Faculty of Informatics and Design*. 2016, Cape Peninsula University of Technology: Cape Town.

[31] [K. A. Wager, F. W. Lee, and J. P. Glaser, "Laws, Regulations, and Standards That Affect Health Care Information Systems", in *Health Care Information Systems: A Practical Approach for Health Care Management* 2017, San Francisco: John Wiley & Sons, 2017, 285 - 322.

[32] T. B. Mahlaola and B. Van Dyk, "Reasons for Picture Archiving and Communication System (PACS) data security breaches: Intentional versus non-intentional breaches". *Health SA Gesondheid*, 21(1): p. 271-279, 2016.

[33] J. R. N. Barrett. "Achieving Data Integrity and Accuracy in the Electronic Health Record". Clinical Analytics 2020 [cited 2020 23 June 2020]; Available from: https://www.symphonycorp.com/clinical-analytics/achieving-data-integrity-and-accuracy-in-ehr/.

[34] S. Bowman, "Impact of electronic health record systems on information integrity: quality and safety implications". *Perspectives in health information management*, 10(Fall): p. 1c-1c, 2013.

[35] M. O. Kim, E. Coiera, and F. Magrabi, "Problems with health information technology and their effects on care delivery and patient outcomes: a systematic review". *Journal of the American Medical Informatics Association*, 24(2): p. 246-250, 2017.

[36] E. Coiera, J. Ash, and M. Berg, "The Unintended Consequences of Health Information Technology Revisited". *Yearbook of Medical Informatics*, 25(01): p. 163-169, 2016.

[37] L. Salahuddin, Z. Ismail, U. R. Hashim, R. R. Raja Ikram, N. H. Ismail, and M. H. Naim @ Mohayat, "Sociotechnical factors influencing unsafe use of hospital information systems: A qualitative study in Malaysian government hospitals". *Health Informatics Journal*, 25(4): p. 1358-1372, 2018.

[38] M. G. Amato, A. Salazar, T.-T. T. Hickman, A. J. L. Quist, L. A. Volk, A. Wright, D. McEvoy, W. Galanter, R. Koppel, B. Loudin, J. Adelman, J. D. McGreevey, D. H. Smith, D. W. Bates, and G. D. Schiff, "Computerized prescriber order entry-related patient safety reports: analysis of 2522 medication errors". *Journal of the American Medical Informatics Association*, 24(2): p. 316-322, 2017.

[39] S. J. Champagin, "Medicare Loses Billions to Billing Errors", in *Proceedings of the Ninth International Conference on Engaged Management Scholarship*. 2019, SSRN eLibrary.

[40] OIG. "Security Gaps May Threaten Electronic Health Records". 2011 06 July 2020; Available from: https://oig.hhs.gov/newsroom/news-releases/2011/security.asp.
[41] F. Xhafa, F. Y. Leu, and L. L. Hung, *Smart Sensors Networks: Communication Technologies and Intelligent Applications.* Intelligent data-centric systems, ed. F. Xhafa. Amsterdam: Academic Press^, 2017.
[42] Y. Zhang, D. S. Myers, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau. "Zettabyte reliability with flexible end-to-end data integrity". in *2013 IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST)*. IEEE, 2013. 1-14.
[43] D. F. Sittig, A. Wright, E. Coiera, F. Magrabi, R. Ratwani, D. W. Bates, and H. Singh, "Current challenges in health information technology–related patient safety". *Health Informatics Journal*, 26(1): p. 181-189, 2018.
[44] HPCSA, "Ethical guidelines for good practice in the health professions". 2019, Health Professions Council for South Africa.
[45] S. Stevenson, "The National Health Act Guide", J. Berger, et al., Editors. 2019: Cape Town, South Africa. p. 207.
[46] B. Zenda, R. Voster, and A. Da Viega, "Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa". *South African Computer Journal*, 32(1): p. 113-132, 2020.
[47] S. Anthony, "Medical Records in South Africa", in *Medical Protection Society Guide*. 2014, Medical Protection Society: South Africa. p. 36.
[48] L. P. Luthuli and T. Kalusopa, "The management of medical records in the context of service delivery in the public sector in KwaZulu-Natal, South Africa: the case of Ngwelezana hospital". *South African Journal of Libraries and Information Science*, 83(2): p. 1-11, 2017.
[49] N. N. Mchunu, "Adequacy of healthcare information systems to support data quality in the public healthcare sector, in the Western Cape, South Africa". 2012, Cape Peninsula University of technology.
[50] M. Ahola, "The Role of Human Errors in Successful Cyber Security Breaches". 2019, usecure: Manchester.
[51] Z. M. Manyisa and E. J. Aswegen, "Factors affecting working conditions in public hosptials: A literature review". *International Journal of Africa Nursing Sciences*, 6(2017): p. 28-38, 2017.
[52] M. J. Mokoena, "Perceptions of professional nurses on the impact of shortage of resources for quality patient care in a public hospital: Limpopo Province". 2017, University of South Africa: South Africa.
[53] J. C. Lubbe and L. Roets, "Nurses' scope of practice and the implication for quality nursing care". *Journal of Nursing Scholarship*, 46(1): p. 58-64, 2014.
[54] P. Barron and A. Padarath, "Twenty years of the South African Health Review". *South African Health Review*, 2017(1): p. 1-10, 2017.
[55] H. K. Nevhutalu, "Patient's rights in South Africa's public health system: Moral-critical perspectives". 2016, Stellenbosch: Stellenbosch University.
[56] J. C. J. Garvey, "Data Integrity: A Structural Approach for Sustainable Outcomes". 2017, FDAnews. p. 46.
[57] M. Botha, A. Botha, and M. Herselman. "Data quality challenges: A content analysis in the e-health domain". in *2014 4th World Congress on Information and Communication Technologies (WICT 2014)*. 2014. 107-112.
[58] Y. Vawda and A. Gray, "South African health review 2018". 2018, Health Systems Trust.
[59] GPW, "Protection of Personal Information ACT, 2013". 2013, Government Printing Works: Pretoria.
[60] HPCSA, "Guidelines on the Keeping of Patient Records", in *Ethical guidelines for good practice in the health care professions*. 2016, Health Professions Council of South Africa: Pretoria.
[61] NDOH, "District Health Management Information System (DHMIS) Policy", N.D.o. Health, Editor. 2011, National Department of Health: South Africa.
[62] B. Babati, "What is data integrity". 2018, Youredi Ltd.
[63] APIC, "Practical risk-based guide for managing data integrity". 2019, Active Pharmaceutical Ingredients Committee. p. 54.