

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Library Philosophy and Practice (e-journal)

Libraries at University of Nebraska-Lincoln

Summer 10-25-2017

The Need for the Establishment of E-records and eHealth Legislation and Policy Framework in the Health Sector in Zimbabwe

Njabulo Bruce Khumalo

National University of Science and Technology - Zimbabwe, njabulobass@gmail.com

Follow this and additional works at: <https://digitalcommons.unl.edu/libphilprac>



Part of the [Collection Development and Management Commons](#), and the [Information Literacy Commons](#)

Khumalo, Njabulo Bruce, "The Need for the Establishment of E-records and eHealth Legislation and Policy Framework in the Health Sector in Zimbabwe" (2017). *Library Philosophy and Practice (e-journal)*. 1662.

<https://digitalcommons.unl.edu/libphilprac/1662>

The Need for the Establishment of E-records and eHealth Legislation and Policy Framework in the Health Sector in Zimbabwe

Njabulo Bruce Khumalo

National University of Science and Technology

Email address: njabulobass@gmail.com

Abstract

Legislation is key to the establishment of eHealth initiatives. Without legislation, authority is not set and the privacy, confidentiality and other threats affecting records and information in electronic platforms are compromised. It is therefore key that legislation for eHealth and e-records be established. Zimbabwe is applying eHealth initiatives in the form of an electronic National Health Information System (NHIS) and other initiatives. However, worrying is the fact that Zimbabwe has not paid attention to the development of legislation and policies for eHealth and e-records management in general. This study sought to make a case for the establishment of e-records and eHealth legislation in order to smoothen the implementation of eHealth systems in the health sector. The study applied a literature review research as literature on eHealth, e-records management and e-health information management was reviewed. The study found that there was no e-records and eHealth legislation in Zimbabwe. The study, thus, recommended the need to enact e-records and eHealth legislation.

Keywords: Legislation, policies, eHealth, health informatics, legal framework.

Subject Headings: Introduction, health information management, eHealth legislation, records management, policy, eHealth legislation. Electronic health records, health information system.

Introduction and Background to the Study

The importance and centrality of policies and legislation in any field cannot be flouted. The advent of technology, though having a lot of benefits, has also brought a multiplicity of challenges which require that legislation and policies be in place. Okello-Obura (2011) remarked that laws have a direct impact on the ways in which governments, organisations and

individuals carry out their daily affairs and they affect the way in which people create and use records since records form the basis for legal evidence. Many records and information management laws were crafted with paper records and information in mind and thus fall short when it comes to e-records. Therefore, the enactment of e-records management legislation shows a country's commitment to e-records management. Mnjama and Wamukoya (2007) suggested that the level of commitment to managing e-records can be gauged by the existence or non-existence of such things as records management policies and procedures. The spreading use of e-health applications in healthcare raises questions about the legal aspects of this development. E-health draws from many fields that include telecommunications, IT, health and medicine and information and records management. Therefore, Bargent, Doktor and Valdev (2005) commented that this means that there are a number of regulatory and other legal issues that govern e-health directly or indirectly. Hence, efforts must not only focus on attending to ICT or telecommunication legislation, but also other concerned areas like records management and archives, censorship, information privacy inter alia. An electronic discussion jointly commissioned by the IRMT and the World Bank (2002) noted that many Commonwealth governments had developed strategies for ICT development, but very few had come up with laws, policies, systems, standards and procedures for managing e- records (Mnjama and Wamukoya, 2007:281).

Bhebhe (2015) noted that the National Archives of Zimbabwe (NAZ) has no proper, written and clear policy on what to do with electronic records produced by the government departments. This is despite the firm belief around the world in general that archivists and national archives, in particular, are the key professionals and institutions, respectively that are responsible for protecting society's documentary memory, whether in paper-based or electronic form. This problem is further highlighted by Miller (2004:6) who lamented that the protection of electronic records is problematic in developing countries due to the weakness of existing legislative, organisational and policy frameworks for the management of electronic records. Bhebhe (2015) also highlights that the challenges faced by the NAZ and government agencies in properly managing electronic records stem from weak archival legislation which has never been updated from 1986 to conclusively cover the management of electronic records. Wamukoya and Mutula (2006) lack of ICT legislation and/or the lack of adequate integration of the legislation with national archival legislation. Young (2008) notes the lack of specific legislative direction with respect to EHRs, despite EHR systems' aggressive uptake in Canada. Young also noted that EHRs were not addressed "with any specificity" within current

legislation in Canada. There is a need to draft legislation, policies and adoption of international health information management standards in order to ensure compliance and good practice (MoHCW Zimbabwe Draft E-health Strategy, 2012-2017). There is need to develop legislation instruments that support eHealth implementation and policies that ensure compliance to agreed protocols and standards (Ministry of Health and Child Welfare, Zimbabwe, 2012).

Problem Statement

Legislation and a policy framework covering eHealth and e-records management in Zimbabwe is lacking yet the Ministry of Health and Child Care among other government departments, continues to implement electronic systems. Such a stance exposes medical records and information to theft, abuse, misuse, breaches of privacy and confidentiality. Without legislation the use of electronic systems has no legal basis and can be abused.

Purpose of the Study

This study sought to make a case for the development and establishment of legislation and policy frameworks for eHealth and e-records management in Zimbabwe.

Research Methodology

This study was a literature review where literature in line with eHealth, e-records management and health information management. Draft health information strategies, reviews, reports, research papers, conference reports and other online documents were reviewed by the researcher through document analysis. The purpose of the literature review was to uncover challenges faced where e-records and eHealth initiatives are introduced without adequate legislation. Furthermore. Literature was also consulted to show how adequate legislation smoothens the implementation of eHealth and e-records management initiatives.. Keywords were identified as highlighted in the keywords section. A retrospective and systematic literature search was conducted online using keywords. Journals, the MoHCC website, and NHIS related reports were the main sources of literature as the researcher conducted an online and physical library search.

Literature Review: Empirical Studies

A key point to take note of in health informatics is that although health information technology (HIT) provides advanced services, it cannot control medical mistakes unless it includes well-defined and consistent policies to manage the use of these systems (Almulhim and Househ,

2012: 377). Kloss (2013) postulated that the efficiency and quality gains from EHRs and other technologies are contingent on the development and enforcement of operational processes and policies that address integrity, accessibility, efficacy and security of data throughout its life cycle. Wamukoya and Mutula (2005:73) noted that at policy level, senior officials and legislators are often unaware of the requirement to manage electronic records over time so that the evidence base of government will be secure and accessible when needed by authorised users. Furthermore, Almulhim and Househ (2012) highlighted that hospitals cannot succeed without applying appropriate health policy to its HIT. Mutiti (2002) discovered that in the ESARBICA region, apart from South Africa, which has put in place measures to manage, destroy and dispose of e-records through a disposal authority, the other countries did not have an explicit policy for managing electronic records. Anon (2010) revealed that many African countries have no policies and strategies to govern e-health initiatives at a national level.

A study conducted by Chikotie (2013:138) highlighted the fact that legislative and regulatory issues in e-health are of concern especially in developing countries. Chikotie (2013) noted that key points from interviews highlighted the need for government laws and policies upholding ICTs in healthcare. Tavakoli and Habibi (2012) also conducted a study whose aim was to recognise laws and procedures pertaining to retention of health records in selected countries and provide a proposed guideline for Iran. This was an applied and descriptive-comparative research on laws and procedures pertaining to retention of medical records in USA, United Kingdom, Australia and Iran that was performed in 2011. The study revealed that, there was complete and transparent record retention schedules in selected counties so that retention situation for adults, minors, emergency, outpatients and deaths records was clearly recommended. However, in Iran, either there were no specific laws and procedures for medical records or they were unspecified which led to confusion for hospitals. Some of the hospitals maintained medical records more than the determined retention period and some of them destroyed them before expiring of essential retention period. In order to optimise the situation of health records retention in Iran, it was necessary to review, correct and complete medical records retention schedules for medical records.

Dostal and Sarek (2011) postulated that the spreading use of the e-Health applications in healthcare raises questions about the legal aspects of this development. In their study, Dostal and Sarek (2011) wanted to look into such questions related to one of the most basic elements of any e-Health solution - electronic health records - in Czech law. The article reviewed the

national legislation related to electronic health records currently in force (which means primarily the Care for Health of the People Act n. 20/1966 Sb.), and to identify possible legal issues that could be preventing the deployment of e-Health Applications. The article showed that the Czech law indeed allowed usage of electronic health records, and set relatively detailed rules in some areas such as what information must be included inside it, and how to archive the data. However, it offered little guidance regarding the question of technical standards for interoperability. The briefness of the Act left a lot of the decisions related to the development of the e-Health applications up to the individual healthcare facilities.

Marutha (2011) conducted a study titled “**Records management in support of service delivery in the public health sector of the Limpopo Province in South Africa**”. Mixed methods were used for the survey and in his conclusion, he noted that hospitals did not have enough guiding documents for the administration of patient records. They had no standard norm for turnaround times for the retrieval of patient medical records in the hospitals. There was also no disposal plan for e-records. The only available records policy was too general and did not entirely cover patient records management and it also did not cover electronic records management. There were no training offered on the policies, procedures, norms and standards for managing records in their institutions. The legislative frameworks for records management were also not accessible to records management officials. They did not know about any of those legislative frameworks.

Kumar, Henseler and Haukaas (2009) conducted a study entitled “**HIPAA’s effects on US healthcare**”. A chronological approach was used to lay out the Act’s effects. Using process flow maps, the pre- and post-Act environment was analysed to discover differences in the two processes. The purpose of the study was to discuss Health Insurance Portability and Accountability Act’s effects on documentation and patient care and future US healthcare options. The findings of this study indicated that by the time the Act was passed, it was already outdated in terms of IT management capabilities. In addition to trying to comply with these outdated practices, the Act’s wording was said to be so vague that hospital staff were not sure with what they are even complying. Kumar, Henseler and Haukaas (2009) recommended that the Act could be improved with some simple changes to wording and updating. The HIPAA affected US healthcare delivery through increased documentation that complicated healthcare process steps. It hindered medical researchers’ ability to get information they need to continue critical research projects. It increased costs owing to poor implementation.

Adebesin, Kotze, van Greunen and Foster (2013) conducted a literature study of e-health standards, their development, and the degree of participation by African countries in the process. The study explored the factors that restricted the adoption of e-health standards by African countries and provided ways of overcoming the barriers. The study revealed that African countries' active participation in e-health standards development is limited to the International Organization for Standardization (ISO), with no evidence of active involvement in other international standards development initiatives. Several factors were found to contribute to limited participation in the development and adoption of e-health standards by African Countries. These barriers included lack of understanding of the importance of standards at a high level, limited participation in standards development, unusable standards, cost barriers to accessing standards, lack of foundational infrastructures, and limited human resource capacity for standard development.

Literature Review

Legislation plays a significant role in records management and from experiences of other countries relevant legislation includes the records and archives laws, e-commerce laws, freedom of information and privacy or data protection laws (Nengomasha, 2009:46). For ehealth records and information initiatives to fully materialise and be adopted, there is a need for comprehensive information management legislation. The Ministry of Health and Child Welfare Zimbabwe (2012: 9) noted that there is need to develop legislation instruments that support eHealth implementation and policies that ensure compliance to agreed protocols and standards. Due to the complexity of health informatics, the Australian College of Health Informatics (2011) emphasised that in drafting health informatics legislation, there must be a consideration of the legislative issues raised by permanent archival or data migration to a different system. In introducing a new way of managing records, the legislative framework or law should be considered first because working against the law may lead to several challenges and problems (Granath, Alariksson and Axelsson, 2004: 31-32). It is therefore prudent that as countries like Zimbabwe and others consider adopting e-records, health informatics and other e-health information and records management initiatives, the subject of enabling legislation and policies be simultaneously addressed.

It has been noted that, there is a propensity to enact legislation which has an impact on records and archives without reference to public records or national archives legislation, in particular

freedom of information and privacy legislation (Roper, 2012). ICT policies and legislation are enacted without the consent and reference to archival concerns and such a stance will negatively affect the long term preservation and security of records in the health sector. In defining the role of a national archival institution, the National Archives and Records Service of South Africa Act (No 43 of 1996, as amended) contains two provisions specifically regarding electronic records systems: that the National Archivist shall determine the conditions subject to which electronic records systems shall be managed, and also the conditions subject to which public records may be electronically reproduced (section 13(2)(b)(ii) and (iii)). As with other public records, the legislation provides that electronic records may not be disposed of without the written authorisation of the National Archivist (section 13(2) (a)). Such legislation places the South African national archival institution at the centre of electronic records creation and management including electronic health records. Mutiti (2001) noted that most countries had no specific legal or administrative framework within which to operate an electronic records management programme and had not begun to address the broader issues involved. Wato (2009) concluded that a lot of countries in the ESARBICA region faced challenges of lack of ICT legislation and poor integration of ICT policy frameworks with national archives. This could hinder effective integration of national archives into the various e-Government drives at a national level (Wato, 2006; Wamukoya and Mutula, 2005).

The NAZ Act (1986) is yet to recognise electronic records and as it stands, NAZ is not empowered by legislation to participate in e-records programmes like e-health and other e-government initiatives. Mutiti (2001) also noted that Botswana National Archives and Records Services was not involved in the drafting of the country's ICT policy. Furthermore, IRMT/World Bank (2003) Global Forum Electronic discussion identified the absence of legislation and policies for the management of information technologies and their products, including electronic records as challenges of managing electronic records. Ketelaar (n.d) emphasised that every archival law should define public records in order "to avoid ambiguity about the scope of the responsibility of the national archives". In Zimbabwe, the involvement of archival institutions and archivists in ehealth platforms needs to be supported by a sound legislative framework that clearly defines the electronic record and the position of NAZ with regards to electronic records. However, Jackson (2008) reasoned that records management law is complex and not well understood.

The IRMT (2002:8) echoed that:

In the absence of legislative imperatives to create authentic, reliable and valid records, the pressure on archives and archivists is increased. Firstly, they need to assess whether archival and records keeping legislation requires revision, always a protracted process. Secondly, they need to be vigilant about whether other legislation in their jurisdiction is pronouncing on record keeping matters and they need to assess whether such legislation is adequate. Thirdly, in the absence of any or adequate legislation, they must identify and employ other tactics to ensure that adequate electronic records are created. This can be achieved through the development of international or national standards or organisational policy. The issues of concern are that such documents may not have the force of legislation and assessing or auditing compliance is a much more difficult task.

Security, Privacy and Confidentiality Issues in eHealth

The application of ICTs in the management of health information has brought about privacy, confidentiality and security concerns. Gajanayake, Lannella and Sahama (2012) stated that security of EHRs is a critical aspect of e-health solutions and the question that arises is whether the data in EHRs are secure enough. As personal health information is digitised, transmitted and mined for effective care provision, new forms of threats to patients' privacy are becoming evident (Appari and Johnson, 2008). Furthermore, Gajanayake, Lannella and Sahama (2012) underscored that a patient's health information may contain sensitive information such as sexual health, mental health, addictions to drug or alcohol and abortions. This makes such a patient demand strong security for their EHRs. The New York Civil Liberties Union (2012:4) propounded that guaranteeing confidentiality and patient control over sensitive health information is critical to the success of electronic health information exchange. In the words of Gajanayake, Lanella and Sahama (2012), healthcare providers have data access requirements and the patients have data privacy requirements which may, in some instances, contradict the access requirements of the healthcare provider. The ease of data analysis in EHRs however increases their demand as different decision makers in the health sectors will need access to EHR to make important decisions. Laudon and Laudon (2005) warned that unprotected electronic records can be hacked by identity thieves or stolen in bulk.

The records manager and archivist participating in eHealth has to consider the high demand for health information by pharmaceutical companies, medical aid and insurance companies, medical service providers inter alia. Dudley (2004) revealed breaches to privacy and

confidentiality in EHR when he highlighted that secondary users have no obligation to respect the doctor-patient relationship characterised by trust and confidentiality, and have both the potential to profit and the resources to access electronic information. Smith and Manna (2004:350) postulated that there have been examples of corporate misuse of private information to deny individuals health or life insurance, jobs and credit. The US National Research Council (NRC) (1997) specified that threats to patient privacy and information security include organisational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting vulnerability of information systems. These threats also include systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC, 1997). Sharpe (2005) expressed that in July 2005, about 57 000 patient records on backup tapes were stolen from a Phoenix based management care company. Moreover, the element of data mining in health informatics though useful, can also threaten the privacy of electronic health records.

Laudon and Laudon (2005) went on to show that third parties can mine electronic records for data to market health products or screen out people as insurance or employment risk, whereas Winkelstein (n.d) added on that data mining may impact confidentiality or lead to discrimination by identifying subgroups. Consumers today have even fewer privacy-protecting options and far less confidence in the privacy of their health information and health decisions (Privacilla, 2004). The health record must be maintained in a manner that follows applicable regulations, accreditation standards, professional practice standards, and legal standards also (AHIMA e-HIM Work Group on Maintaining the Legal EHR, 2005). Due to the dispersed nature of health IT systems that contain or comprise the record of care, healthcare organisations must establish governance processes that include record management policies, retention schedules, destruction procedures, privacy and security practices, and custodianship or stewardship roles and functions (Dougherty and Washington, 2010). In light of modern medical practice' and the growth of third-party insurers, individuals no longer possess a reasonable expectation that their histories will remain completely confidential (Lichtblau, 2004). The Ministry of Health and Child Welfare Zimbabwe (2012:24) emphasised that health practitioners and other stakeholders who will be in possession of patient information should understand and always protect the patient privacy, and the confidentiality of such information should be governed by statutes and legal instruments. A new report reveals that in 2013, the number of protected health information (PHI) breaches were up 138 percent from 2012, with

199 incidents of breaches of PHI reported to HHS impacting over 7 million patient records (Penna, 2014). The theft of a password-protected unencrypted desktop computer from the Albany, Ga.-based Phoebe Putney Memorial Hospital has compromised the information of 6,777 patients (Leventhal, 2014).

On September 20, 2010, a computer flash drive containing the names, addresses, social security numbers (SSNs), and protected health information (PHI) of 280,000 Medicaid members was stolen from the corporate offices of a health plan (Von Bergen, 2011). On May 3, 2006, a laptop and disc containing personal health information (names, SSNs, date of birth, and other information) for 26.5 million veterans was stolen from a United States of Veterans Administration (VA) America employee's home (Pritts, 2005). Security, privacy and confidentiality of health records created and managed in electronic platforms have been a cause for concern, and in trying to address these and other issues, the records management field has tried to come up with functional requirements for electronic records.

Conclusion and Recommendations: The Need to Establish E-records and eHealth Legislation in Zimbabwe

Legislation and policies are key especially in such areas like eHealth which are driven by ICTs and are prone to a lot of britches of privacy, technological obsolescence, the need to share information across different health facilities and practitioners. In a country like Zimbabwe, which is slowly adopting different technologies for use in health information and records management, it is key that the regulatory and policy framework be strengthened to avoid challenges which are usually tied to these technologies. The Ministry of Health and Child Care, Zimbabwe (2012) noted that there is need to develop legislation instruments that support eHealth implementation and policies that ensure compliance to agreed protocols and standards.

Policies define priorities and provide a guiding framework within which all stakeholders operate (WHO, Health Metrics Network, 2008b). The health sector in Zimbabwe is divided into two, which is, the private and public health care systems and if e-Health systems will be effective, there is need for uniformity and the need for sharing information across these sectors. Legislation and regulation are particularly significant in relation to the ability of the national HIS to draw upon data from both the private and public health services, as well as non-health sectors (World Health Organisation, Health Metrics Network, 2008a:17). Particular attention

to legal and regulatory issues is needed to ensure that non-state health-care providers are integral to the national HIS, through the use of accreditation where appropriate (World Health Organisation, Health Metrics Network, 2008a:17). Legislation enhances access to data from all sources including the private and non-governmental health institutions (WHO, Health Metrics Network, 2008b). Without legislation there is no compliance to talk about and thus private players do not have any obligation to coordinate and work with public health facilities. The lack of appropriate legislation contributes to the current challenges experienced in collecting data from private health institutions (Ministry of Health Botswana, 2009). Private hospitals provide very limited information while private practitioners and non-governmental organizations do not report any data (Ministry of Health Botswana, 2009).

Policies can thus provide guidance on which all these sectors can operate and avoid malpractice and substandard eHealth systems. Furthermore, policies may be drafted and put in place, but without legislation in place, compliance becomes a challenge as there will not be any clause legally binding stakeholders in the health sector. Countries should review their health legislation and promulgate new legislation and regulations as needed to ensure that their policy intent is supported and that legislative gaps are filled (Africa Health Strategy, 2007-2015). It is therefore prudent that eHealth supporting legislation be drafted in Zimbabwe in order to see to it that policies are supported and all stakeholders have common ground. According to the Africa Health Strategy (2007-2015) Legislation and consequent regulation are key tools in giving effect to policy.

The World Health Organisation, Health Metrics Network (2008a:17) highlights that the legal and regulatory contexts within which health information is generated and used enable mechanisms to be established to ensure data availability, exchange, quality and sharing. Without such legislation, the benefits of technology which include sharing of data across facilities and between health and medical practitioners becomes a nightmare. The justification for investing in technologies in health information ad records management has been that of information sharing and without legislation in place, this becomes a challenge. Furthermore, Legal and policy guidance is also needed, for example, to elaborate the specifications for electronic access and to protect confidentiality (World Health Organisation, Health Metrics Network (2008a:17). Legislation will demarcate the level of access and confidentiality bearing in mind that a lot of players and stakeholders want access to health information whereas

patients may not want their health information to be accessible to all and sundry. Legislation will therefore have to strike a balance in this case and see to it that patients are protected and that necessary players are afforded the privileges of accessing certain information or data.

Another important aspect in eHealth information and records management is custody. It is key that there be specifications as to which organisations, stakeholders and officers are responsible for archiving and or the custody of e-records and information in the health sector. The Pan Canadian Health Information Privacy Group (2012) states that legislation also highlights health information custodian to describe the entity accountable in legislation for the personal health information in its custody and/or under its control. Without legislation, there is no accountability as no one is designated the role of keeping custody of records and information in the health sector. Therefore, e-health records and information can be compromised, deleted, tempered with or even lost without legislation in place. Furthermore, the management of health records and information in eHealth platforms calls for an interdisciplinary approach and different stakeholders and professionals have to pool their expertise together and link up to ensure the long term preservation of such records and information. Legislation will provide that link as Roper and Miller (2009) highlight that if legislation is well designed, it will give the head of the records and archives institution overall responsibility for hospital records and will make the heads of hospital records services professionally accountable to him or her.

Legislation also enables different stakeholders in eHealth to authoritatively carry out their tasks and duties. For stakeholders like national archival institutions what are also key players in e-Health, archives legislation enables archival institutions to operate with authority in its dealings with other public institutions and with legislation in place, archival institutions have the authority to protect and preserve the nation's records and archives (Kashekwa, nd). Legislation further sets out the responsibilities of the heads of public offices and those of the Director of the archival institution (Barata, Piers and Routledge, 2001). Key stakeholders in eHealth will be left out if care is not taken to have legislation to highlight roles and responsibilities of different players in eHealth. It is also on record that without legislation in eHealth, some stakeholders will overtake roles they are not qualified to take.

Legislation also protects privacy, confidentiality and autonomy in eHealth platforms. EHRs can threaten autonomy if proper protections are not put in legislation to prevent personal health

data from being used in secondary ways in public health research or by curious entities, such as insurance companies (Goodman, 2012). Health information must be protected from secondary use by legislation. Data mining makes it possible to deduce trends, patterns and derive other data which is very useful for insurance companies, marketers, health practitioners, pharmaceutical companies and other players. The presence of legislation will at most be critical in stopping such secondary users from accessing patient information and records.

Technology is very dynamic and new technological products and systems are ever being released into market. Some of these systems are proprietary whereas others are open. With proprietary systems, the exchange, sharing and migration of information from one system to another is usually a challenge as the form, context and content may be lost in the process of migration. This is a problem especially when considering archiving or the long term preservation of records and information in the health sector. Adebessin et al (2013) highlights that there should be legislation and policies that address e-health interoperability. It is prudent that in Zimbabwe, eHealth legislation be drafted to address such issues like interoperability. If different players in the private sector continue making use of various proprietary systems, sharing of data and information or even linking with the National Health Information system will be a challenge. Legislation will thus specify on how interoperability will be achieved, either by the use of open systems and any other means. The existence of a legal and policy framework consistent with international standards, enhances confidence in the integrity of results. A legal framework can also define the ethical parameters for data collection, and information dissemination and use. The health information policy framework should identify the main actors and coordinating mechanisms, ensure links to programme monitoring, and identify accountability mechanisms (World Health Organisation, Health Metrics Network, 2008a).

References

- Adebesin, F., Foster, R., Kotze, P. and van Greunen, D. (2013). A review of interoperability standards in e-Health and imperatives for their adoption in Africa. *SACJ*, 50.
- Africa Health Strategy. (2007-2015). Third session of the African Union Conference on Ministers of Health Johannesburg, South Africa, 9– 13 APRIL 2007.
- Almulhin, D. A and Househ, M. S. (2012). A perspective on the influence of health policy on health technology use within the Arab world. *Journal of Health Informatics in Developing Countries* 6(1): 375-384.
- Appari, A. and Johnson, M. E. (2008). *Information security and privacy in healthcare: Current state of research*. (Online). Available at: <http://www.ht://www.lse.ac.uk/management/documents/Electronic-Health-Privacy.pdf> (Accessed on 23 February 2014)
- Australian College of Health Informatics. (2011). *Response to request for comment on the personally controlled electronic health record (PCEHR). SYSTEM: Legislation issues paper*. (Online). Available at: http://www.achi.org.au/docs/ACHI_Response_PCEHR_Legislation_V1.0.pdf (Accessed on 04 October 2013).
- Australian Government Department of Health and Ageing. (2012). *Getting ready for e-health records: Medicare Locals Support*. (Online). Available at: <http://www.amlalliance.com.au/medicare-localsupport/ehealth/ehealthresources/?a45234> (Accessed on 12 July 2013).
- Australian Standard AS 4390. *Standards Australia*, (1996). (Online). Available at: www.territoryrecords.act.gov.au (Accessed on 23 January 2015).
- Barata, Kemberly; Cain, Piers and Routledge (2001) *Principles and Practices in Managing Financial Records: A Reference Model and Assessment Tool*. Available at <http://www.irmt.org> (Accessed on 12 July 2013).
- Bargent, D. C., Doktor, R. and Valdez, M. (2005). *Human and organisational dynamics in e-health*. Abingdon: Radcliff Publishing.
- Bhebhe, S. (2015). Contemporary diplomatics of the civil and deceased estate case files found at the national archives of Zimbabwe", *Records Management Journal*, 25(1): 107 – 120.
- Chikotie, T. T. (2013). ICTs and public healthcare service delivery in a developing country context: Critical factors towards addressing the health divide. *Journal of Health Informatics in Africa* 1(1-62): 133-140.

Dostal, O. and Sarek, M. (2012). Support for electronic health records in Czech law. *European Journal of Biomedical Informatics* 8(2): (Online). Available at: <http://www.ejbi.org/img/ejbi/2012/2/Dostalen.pdf> (Accessed on 22 May 2014).

Dougherty, M and Washington, L. (2010). Still seeking the legal EHR: The rush for electronic records increases, the records management question remains. *Journal of AHIMA* 81(2): 42- 45.

Dudley, G. (2004). *Electronic records, patient confidentiality and the impact of HIPAA*. Marieta. Lion heart Publishing. (Online). Available at: <http://www.psqh.com/octdec04/dudley.html> (Accessed on 22 July 2016).

Gajanayake, R., Lanella, R and Sahama, T. (2012). Privacy oriented access control for electronic health records. (Online). Available at: <http://www.dig.csail.mit.edu/2012.pdf> (Accessed on 15 January 2016).

Goodman, P. (2012). *Electronic health record regulation in Canada: What the patient experience reveals about the pursuit of legislative harmonization*. Masters Thesis: The University of Western Ontario London, Ontario, Canada

Granath, P. Alariksson, S. and Axelsson, S. (2004). Creating a system for public information: the Swedish aid agency's transformation to electronic administration. *Records Management Journal* 14(1):25-32.

International Records Management Trust/World Bank. (2003). Evidence-based governance in the electronic age. *Global Forum Electronic Discussions*. Summary of Discussion One: Information Technology, Electronic Records, and Record Keeping. (Online). Available at: http://irmt.org/documents/research_reports/e_discussions/IRMT_ediss_inf_tech.pdf (Accessed on 18 June 2015).

Jackson, K. M. (2009). *Electronic health records and public health informatics: Electronic health records and public health informatics*. New York: Old Post Publishing.

Jackson, R. (2008). Recordkeeping standards confuse users and vendors. (Online). Available at: http://www.computerworld.co.nz/article/496426/recordkeeping_standards_confuse_usersvendors (Accessed on 31 January 2014).

Kashekwa, K. (nd). *Archival Legislation and the Management of Public Records in Sub-Saharan Africa: The Case of the National Archives Act of Zambia*. *Zambia Library Association Journal*

Ketelaar, E. (1989). *Archival and records management legislation and regulations*. (Online). Available at: <http://www.unesco.org/webworld/ramp/html/r9006e/r9006e0i.htm> (Accessed on 12 January 2014).

Kumar, S., Henseler, A. and Haukaas, D. (2007). HIPAA's effects on US healthcare. *International Journal of Healthcare Quality Assurance* 22(2): 183-197. Kvale S. 1995. The social construct of validity. *Qualitative Inquiry* 1:19-40.

Laudon, K. C and Laudon, J. P. (2005). Essentials of management information systems: Managing the digital firm. 6th Ed. New York: Pearson Education.

Leventhal, R. (2014). Security breach at government hospitals affects 6700 patients. (Online). Available at: <http://www.healthcare-informatics.com/category/technology/privacysecurity>. (Accessed on 12 November 2016).

Marutha, N.S. (2011). Records management in support of service delivery in the public health sector of the Limpopo province in South Africa. PhD Thesis. University of South Africa.

Miller, L. (2004). Authenticity of electronic records: a report prepared for UNESCO and the international council on archives”, available at: www.ncd.matf.bg.ac.rs/standards/archivist.pdf

Ministry of Health Botswana. (2008). Situational analysis: Health information/monitoring & evaluation within the health service delivery setup: 2008. Ministry of Health Botswana: Gaborone.

Ministry of Health and Child Welfare, Zimbabwe. (2012). Zimbabwe’s Draft E-health Strategy 2012-2017. Retrieved June 4, 2016, from http://www.who.int/goe/policies/countries/zwe_ehealth.pdf

Mnjama, N. M. (2005). “Archival landscape in Eastern and Southern Africa”. Library Management 26(8/9):457-470. (Online). Available at: <http://www.emeraldinsight.com/doi/full/10.1108/01435120510631747> (Accessed on 22 January 2014).

Mutiti, N. (2002). Computerisation of archives and records in the ESARBICA region. ESARBICA Journal 2: 114-119.

Mutiti, N. 2001. The challenges of managing electronic records in the ESARBICA region. ESARBICA Journal 20(3): 57-61.

Nengomasha, C. T. (2009). A study of electronic records management in the Namibian public service in the context of e-governance. PhD Thesis: University of Namibia. (Online). Available at: <http://www.repository.unam.na/bitstream/handle/11070/447/nengomasha2009.pdf>? (Accessed on 12 June 2016).

New York Civil Liberties Union. (2012). Protecting patient privacy: Strategies for regulating electronic health records exchange. New York: New York Civil Liberties Union.

Okello-Obura, C. (2011). Records and archives legal and policy frameworks in Uganda. Library Philosophy and Practice (e-journal). (Online). Available at: <http://digitalcommons.unl.edu/cgi/viewcontent.cgi?> (Accessed on 14 March 2016).

Pan Canadian Health Information Privacy Group. (2012). Privacy and EHR information flows in Canada: Common understandings of the Pan-Canadian Health Information Privacy Group. Pan-Canadian Health Information Privacy Group: Canada.

Perna, G. (2014). Report: Breaches up 138 percent in 2013. (Online). Available at: <http://www.healthcareinformatics.com/category/technology/privacysecurity> . (Accessed on 21 November 2016).

Pritts, J. L. (2005). Testimony before the United States House of Representatives Committee on ways and means subcommittee on health care information technology: Harmonising laws governing the confidentiality of healthcare information. (Online). Available at: <http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg26387/html> (Accessed on 17 January 2016).

Roper, M. (2012). Study of legislation affecting records and archives in Commonwealth countries. (Online). Available at: <http://www.acarm.org/view.asp?item> (Accessed on 12 March 2016).

Roper, M and Miller, L. Ed. (1999). *Managing public sector records: a study programme: managing hospital records*. London: International Records Management Trust. [Online] Also available from: <http://www.irm.org/Images/documents/edu-training/public-sector> (Accessed on 12 March 2016).

Sharpe, V. (2005). Perspective: Privacy and security for electronic health records. (Online). Available at: <http://www.medscape.com/viewarticle/517403> (Accessed on 13 February 2016).

Smith, A. D. and Manna, D. R. (2004). Exploring the trust factor in e-medicine. *Online Information Review* 28(5): 346-355.

Tavakoli, N and Habibi, M. R. (2012). A comparative study of laws and procedures pertaining to the medical records retention in selected countries. *ACTA Informatica Medica* 20(3): 174-179.

Wamukoya, J. and Mutula, S. M. (2006). Capacity-building requirements for e-records management: The case in East and Southern Africa. *Records Management Journal*, 15(2): 71-79.

Wato, R. (2004). Challenges of archival electronic records: The imminent dangers of a dark age. *ESARBICA Journal*, 23: 108-122.

Winkelstein, P. S. (nd). *Ethical and social challenges of electronic health information*. New York: Buffalo.

World Health Organisation, Health Metrics Network. (2008a). Assessing the National Health Information System: An Assessment Tool VERSION 4.00. World Health Organisation: Geneva.

World Health Organisation. Health Metrics Network: (2008b). Framework and standards for country health information systems 2nd ed.: World Health Organization. 2008.

Young, D. (2008). Security of electronic health records: does current legislation adequately protect?