

Winter 6-15-2017

Records Risk Assessment at a Hospital in Zimbabwe

Njabulo Bruce Khumalo Mr
University of Venda, charitiebals@gmail.com

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

 Part of the [Library and Information Science Commons](#)

Khumalo, Njabulo Bruce Mr, "Records Risk Assessment at a Hospital in Zimbabwe" (2017). *Library Philosophy and Practice (e-journal)*. 1558.

<http://digitalcommons.unl.edu/libphilprac/1558>

Records Risk Assessment at a Hospital in Zimbabwe

Njabulo Bruce Khumalo/ Gay Nyirenda

National University of Science and Technology/ Mater Dei Hospital

Email: njabulobass@gmail.com

Email: gnyirenda08@gmail.com

Abstract

Many organisations usually do not value records management until a time when disaster strikes and records are destroyed. In most institutions, there is a lack of preparedness as there are no records risk assessments and records management systems are not assessed to find how they are performing. Without records risk assessment activities in especially hospitals, records will continue to deteriorate, be lost or even accessed by unauthorised people. Without proper records risk assessments, disasters are likely to strike and destroy records which are the basis for business transactions, continuity and evidence. Purpose of the Study: This study will seek to conduct a records risk assessment on a hospital in Zimbabwe with the aim to finding how its records management system is efficient and effective. Methodology: This study will be qualitative in nature and a case study research design applied, where the case will be the hospital's records management system. The University of Technology Sydney Records Management Programme Risk Assessment Tool will be used in assessing risks. The sampling applied in this study will be purposive as the researchers know the research participants who are knowledgeable on the subject matter under-study. Findings: This study will conclude that records at the hospital are facing a number of risks which are likely to cost the hospital in cases of litigation. Practical Implications: This study will go a long way in pointing to the strengths and weaknesses of the hospital's records management programme. The hospital can then seek to improve its records management system based on the findings of this study. Originality of the Study: Records management programme risk assessments have been done in other universities and organisation, yet one has not been conducted in the hospital which is being studied in this case. This will be a research paper.

Keywords: risk assessment, disaster, preparedness, system, hospital. Litigation.

Introduction

Records are at the heartbeat of the healthcare delivery system which depends on the availability and timely provision of records. The most important reason for physicians to maintain accurate, credible medical records is that good documentation protects patients and medical records contain information required to inform physicians of past and present treatment decisions, and to provide evidence that such care was appropriate in all respects

(The Medical Insurance Exchange of California, 2008). Without records, lives of patients are at stake, whereas physicians' practice may suffer and be lose credibility and efficiency. The Medical Protection Society of South Africa (2014) postulates that there is a need to secure the integrity and confidentiality of personal information, prevent loss of, damage to or unauthorised destruction of or unlawful processing or access to personal information. Due to the nature of their work, medical and healthcare practitioners may face litigation due to medical procedures gone bad and other glitches. Many malpractice claims result in a victory for the plaintiff because of the poor quality of medical records, even in cases in which appropriate medical care was provided. Maintaining adequate, defensible medical records need not be a chore (The Medical Insurance Exchange of California, 2008). Therefore, up to date records need be managed by healthcare facilities in order to protect the lives of patients, prove their informed decision making and the following of standard modus operandi in medical procedures. The importance of records in the health sector therefore calls for measures to be put in place to guarantee that records are managed meticulously to avoid losses, theft, and other disasters. One of the most important measures is the clear identification of what is most at risk, and of what truly merits fully protection (Penn, Pennix and Coulson, 1994:146). Risk assessment is an essential part of risk management and is the overall process of risk identification, risk analysis and risk evaluation (ISO 31000: 2009).

Literature Review

Records risk assessments are critical to ensure that any healthcare facilities have proper records management systems and that they detect possible disasters and apply measures to ensure that records are secure and safe from harm. The Office of the National for Health Information Technology Coordinator (USA) (2015) states that the risk assessment process identifies potential security weaknesses and flaws and there is a need to periodically conduct such assessments as there might be changing environments and new challenges and developments. The importance of records risk assessment is highlighted by the Medical Insurance Exchange of California (2008) which states that nothing is more devastating to an innocent physician's defence against the allegations of medical malpractice than an inaccurate, illegible or skimpy record, except for a record which has been changed after the fact, and therefore inevitably compromises the otherwise defensible case. Therefore, Emery (nd) highlights that organizations, both large and small, fail to take effective measures to manage and protect their documents and records to mitigate the risks of hurricanes, terrorism attacks, extended power outages and other business interruptions. Risk assessment assists

organizations to evaluate and assess the adequacy of controls in relation to dealing with identified threats (Wold and Shriver, 1997). Poba- Nzaou (2016) notes that the risk exposure as well as risk management are influenced by contextual factors; and these factors increase or decrease the exposure to risk. It implicitly assumes that risk management can be understood through the alignment or fit between a hospital's level of exposure to risk and its risk management profile.

The advent of technology has greatly enhanced health records and information management it has become easy to share e-records and information between different health practitioners and healthcare facilities. However, ICTs are not exempt from risks as the Canadian Medical Protective Association (2014) opined that new technologies should not be adopted or used before the privacy and security risks are fully analyzed, along with the measures that should be taken to enable physicians to comply with privacy legislation. EHR have not always generated the expected, later benefits. Hence, it is not surprising to find that, "in the excitement over [EHR], the potential risks associated with it have received less attention" (Mangalmurti, Murtagh and Mello (2010), Daly (2015) The failure of an EHR implementation or the poor management of EHR risk associated with its use may hamper a hospital's ability to generate potential benefits in addition to putting patients' lives at risk and wasting scarce resources. In a broad sense, the poor management of EHR risk has resulted in a high level of dissatisfaction of hospitals with their EHR systems to the extent that recent surveys have reported that about 20% of hospitals want to retire their current EHR and switch to another system.

The Medical Protection Society of South Africa (2014) further underscores that the person in charge of a health establishment in possession of a user's health records must set up control measures to prevent unauthorised access to those records and to the storage facility in which, or system by which, records are kept.

Risks Affecting Records

Records are prone to a number of disasters, which can be manmade and natural, and records risk assessments have to identify such disasters and risks. Some risks to records as highlighted by Ndenje-Sichalwe (2010) may include storage conditions that are unsuitable for the media stored, and by the natural decay of materials and as a result disaster planning and security control are vital to the preservation and protection of records. It therefore becomes

imperative that records storage areas provide stable and conducive environments which do not risk the long term preservation of records. Royal Cornwall Hospitals Trust (2011) records should be identified whenever possible at the point of creation, whether born digital or from other media. This enables the organisation to identify, capture, and control those records that are vital records or with archival or long-term value, eliminating any risk to their longevity or integrity. Records can also be affected by cockroaches, termites, booklice, bookworms, rats, mice seem to be the pests that were experienced in the record storage area (Kalusopa, 2011).

Records management personnel have to be in the lookout for all kinds of disasters. Lihoma (2012) film archive collection deteriorated beyond use and was disposed of due to poor storage conditions while some archives have been ravaged by termites. Kalusopa (2011) highlighted that bomb threats, explosions, floods, food and drink in storage area, pest infestation, leaking roof, sabotage, unauthorised intrusion and computer system failure are some risks to records. Regardless of format, patient records are subject to the risk of inappropriate access and the sheer volume of records increases the likelihood that records are lost because they are incorrectly filed or never returned to the file room. Ndenje-Sechalwe (2010) further notes that records are particularly at risk from light damage which usually affects photographs, newspapers and manuscript inks should be identified, and their exposure to visible and ultraviolet light should be minimized.

There has to be records management controls in the form of policies and procedural manuals to facilitate the retention of records for as long as they are needed. Chaterera (2016:129) highlighted that the absence of a retention and disposal schedules implies that important public records are at risk of being destroyed prematurely while ephemeral records are retained longer than necessary. Furthermore, without standards especially in digital information and recordkeeping platforms, there are risks that the records and information created therein might not be accessible in the future. Health information is confidential and must therefore be protected and or safeguarded against unauthorised access. The Health Practitioners Council of South Africa (2006) states that unauthorised use or retransmission of confidential patient information have been identified as some of the potential risks to records.

Furthermore, the healthcare system's move to electronic healthcare records has created new exposures as records are now more easily accessed by consultants, vendors and other third parties for efficient operation. Additionally, healthcare organizations face exposure to cyber

risks that could have significant impacts on their operations, including shutting down critical, health-related systems (Doherty and Carino, 2015). The Queensland State Archive (2010) stated that without a strategic digital archiving approach, poor information management practices across the lifecycle of digital information means that records are at risk of losing their trustworthiness, integrity and authenticity, or simply becoming lost or inaccessible. Electronic records depend upon computing technologies that have notoriously short lifecycles and this means that during the life of an average medical record, the computing technologies will have undergone multiple generational changes as replacement parts become unavailable and while operating systems and database platforms lose vendor support.

The Medical Protection Society of South Africa (2014) also notes that paper records in particular can be easily damaged by moisture, water, fire and insects and unlike electronic records, it is not feasible to create up-to date copies against the chance destruction of the originals. Your paper records are therefore not only vulnerable, but irreplaceable. Moreover, vital records have to be identified and secured as the hospital cannot operate without them. Royal Cornwall Hospitals Trust (2011) highlights that unidentified vital records increase our liability at times of risk assessment and can equate to the Trust paying out in both financial and human terms in the event of a major disaster

Statement of the Problem

Records are faced with a number of risks which usually are unidentified until such a time when disaster strikes, records are stolen, go missing, or chewed and cannot be salvaged. Hospitals may also not have purpose built structures for records storage and hence records are prone to water pipe leaks, termites, floods and other possible disasters. The major challenge is that such risk go unidentified and organisations like hospitals are struck by disasters and fail to respond or manage disasters. Not conducting records risk assessments jeopardises health records.

Purpose of the Study

This study sought to conduct a records risk assessment for a private hospital in Bulawayo Zimbabwe. Such an assessment would go a long way in identifying possible risks which can affect the hospital's records.

Research Methodology

This study was quantitative as a records risk assessment tool was used. A closed ended questionnaire derived from the University of Technology Sydney Records Risk Assessment tool, was distributed to the hospital's records management personnel. A quantitative case study research design was applied and all 3 members of staff managing health records in the hospital were the population of the study.

Findings of the Study

The findings of the study are presented under four subheadings which are; Environmental Conditions, Human Error, Procedures, Policy, Security, Storage and Implementation of Disaster Planning. Data was gathered from 3 respondents who are responsible from managing records in the hospital. These respondents were responsible for running the hospital's 3 small records storage areas.

Summary of the Findings: Environmental Conditions

Risk	Is the Hospital Affected by this Risk (YES/NO)	Number of Respondents identifying the Risk	Likelihood of Risk Affecting the Hospital
Temperature Fluctuations	YES-	3 (100%) respondents	High
Dust	YES	3	High
Sunlight	NO YES	2 (67 %) Not affected 1 (33%) respondent affected	Medium Low
Pest and Insects Infestation	YES NO	2 (67%) affected 1 (33%) Not affected	High Low
Chewed Boxes and Records	YES	3 (100%) affected	High
Magnetic Fields Affecting E-records	NO	0 (0%) affected	Low
Damp, Mouldy, Flooding Areas	NO	0 (0%) affected	Low

Assessment of Environmental Conditions

It is essential that records be stored in areas whose temperatures are stable and do not fluctuate. Fluctuating temperatures lead to the deterioration of records and as such, is advisable that records rooms be air conditioned to avoid fluctuations in temperatures. The standard temperatures and relative humidity for paper records retained for up to 30 years is 15-27 °C and 30-60% RH, while for photo, magnetic and optical records is 19-21 °C and 47.5-52.5% RH. The first assessment question sought to find out if there are fluctuating temperatures where hospital records are kept question The 3 respondents in this study highlighted that their records storage areas were stored in areas subjected to high and fluctuating temperatures. The 3 (100%) respondents highlighted that the likelihood of fluctuations in temperatures was high. The data also revealed that there were no air conditioners in all of the hospital's records rooms.

Dust is also harmful to records and as such records storage areas must not be exposed to excessive dust. The data in this study revealed that records were being stored in areas subjected to excessive dust levels. The 3 respondents highlighted that the likelihood of excessive dust was high in their work environments and the likelihood of dust affecting records was also high. Sunlight is also harmful to records and thus, records rooms or offices need to have dimmers or any other material that can avoid direct sunlight. 2 of the respondents highlighted that their records storage areas were not exposed to direct sunlight and the likelihood of sunlight affecting their records was low, whereas, 1 respondent highlighted that records in his unit were exposed to direct sunlight as his office windows did not have dimmers and the likelihood of sunlight affecting records was medium.

Pests and insects can damage records over time and infest other areas when records are moved. In this study 2 of the respondents highlighted that their records storage areas had signs of infestation whose likelihood was high, whereas the remaining 1 respondent stated that there were no signs of infestation in the records storage area and the likelihood of pests and insects affecting records was low.

Respondents were further required to highlight if their work environment had any evidence of mice or other vermin. Chewed boxes and records are some of the signs of the presence of mice. All the 3 respondents highlighted that there was evidence of mice in records storage

areas as evidenced by chewed boxes and records. Furthermore, the data showed that the likelihood of records being chewed was high as highlighted by the 3 respondents.

Hospitals have adopted e-health information management systems, and thus, respondents were asked if areas in which they stored e-records were affected by magnetic fields and all the 3 responses pointed to the fact that e-records were not affected by magnetic fields and the likelihood of magnetic fields affecting e-records in the hospital was low. The records risk assessment also sought to find out if areas in which records were stored were damp, mouldy or subjected to flooding. All the 3 responses pointed to the fact that the hospital's records storage areas were not affected by moulding, dampness and floods. The likelihood of these disasters affecting the hospital was low.

Overall Assessment of Environmental Conditions

Under environmental conditions, it can be concluded that temperature fluctuations, dust, sunlight, pest and insect infestations and chewed boxes were some of the risks which could possibly affect the hospital's records. However, the hospital was not affected by magnetic fields affecting e-records and damp, mouldy and flooding areas.

Summary Conclusions for Human Error, Procedures, Policy

The study also assessed risks associated with human error, procedures and policy in line with the hospital's records management. The findings of the study are presented below.

Risk	Is the Hospital Affected by this Risk (YES/NO)	Number of Respondents identifying the Risk	Likelihood of Risk Affecting the Hospital
Absence of Records Management System	YES	3 (100%) All sections did not have records management system in place	High
e-records and information kept without printed hard copies	NO	0 (0%) All sections were making copies of e-records and information	Low

Original Contracts and Agreements without Copies	NO	0 (0%) All sections not affected	Low
Signs of Smoking in Records Storage Areas	NO	0 (0%) All sections not affected	Low
Deliberate Deletion of Records	NO	0 (0%) All sections not affected	Low
Accidental Deletion of Records	NO YES	2 (67 %) of the respondents not affected 1 (33 %) affected	Low Medium
Records Taken Home and Lost	NO	0 (0%) affected	Low
Records lost due to staff relocations/ office movements	NO	0 (0%) affected	Low
Records Requested and Never Returned	YES	3 (100%) affected	High

Human Error, Procedures, Policy

In order for records management activities to be executed well, there is a need for a records management system and thus respondents were asked if the hospital had any formal records management system in place. All the 3 responses pointed to the fact that there was no records management system in use at the hospital. Respondents were further asked to highlight if there were any official records which were being kept in electronic or technology dependent formats without copies kept in official hard copy files. The data showed that all official records in electronic formats had hard copies which were filed and kept as backup.

Contracts and agreements are key records in any organisation and they must be kept safely to avoid litigation and as evidence in case the hospital is required to defend itself in legal battles. The assessment tool therefore sought to establish if the records management units were keeping original contracts or agreements locally instead of lodging them with the hospital's main administration unit. The 3 respondents highlighted that their units were not keeping any original contracts and agreements as these were being managed by the hospital's

management and administration. These respondents highlighted that they only kept copies of such records.

Fire is also another disaster which is capable of destroying records and thus caution must be taken to ensure that registries or records storage areas are not susceptible to fire. Such areas have to be “no smoking areas” within any organisation. All the 3 respondents highlighted that the records storage areas at their places of work had policies against smoking and thus there was no smoking close to records storage areas. In some cases, records are deliberately deleted or destroyed to avert disciplinary actions, crimes and other charges whose deliberations need records as evidence. The data showed that the hospital had never experienced cases of the deliberate deletion or destruction of records in their sections. The data also showed that 2 of the respondents highlighted that there were no cases of accidental destruction of records in their sections. However, the remaining respondent highlighted that there had been cases of accidental destruction or deletion of records in her section.

Records are always being requested for especially in hospital environments where healthcare is dependent on the availability of records as points of reference. In some cases, some officials may take records home and in the process lose such records. However, when asked if records had been lost by officials who had taken them home, the 3 respondents highlighted that they had not lost any records taken home by officials. These respondents also highlighted that they had not lost any records due to staff relocations or office movements. However, all 3 respondents stated that they had lost records due to staff members who had requested for the records and never returned them. All the 3 respondents highlighted that they had had cases where records were borrowed and never returned by staff members who left the hospital employ.

Overall Summary Conclusions for Human Error, Procedures and Policy Risks

The findings of the study showed that the hospital was facing records management challenges due to the absence of any records management system, a few cases of accidentally deleted records and records requested by officers in the hospital and never returned. The records sections had had cases of records requested for and never returned. On a positive note, it can be concluded that the hospital had backups as e-records were printed resulting in hard copies filed, and the records management sections were not keeping copies of agreements and contracts. Furthermore, there were no signs of smoking, and there were no cases of deliberate

deletion of records from computers. The assessment also revealed that the hospital had not come across any cases of records taken home and lost and had never had cases of records lost due to staff relocations/ office movements. However, the study revealed that there had been a case of accidental destruction of records.

Summary of Findings: Security

Risk	Is the Hospital Affected by this Risk (YES/NO)	Respondents identifying the Risk	Likelihood of Risk Affecting the Hospital
Access to Current and Semi Current Records by Unauthorised personnel	YES	3 (100%) affected	High
Access to Archives by Unauthorised personnel	NO	0 (0%) affected	Low

Findings: Security

Due to the sensitivity of records housed in hospitals, there is a need to ensure the security of such records against unauthorised access. This section of the assessment sought to find out if there were cases of access to records by unauthorised members of staff. All the 3 respondents highlighted that they had had cases of access to records by unauthorised members of staff. However, all the 3 respondents highlighted that the hospital's archive was not accessible to unauthorised personnel. Therefore, it emerged that current and semi current records were accessible to unauthorised personnel, whereas archives were secured and inaccessible. These respondents also highlighted that health information management databases were not accessible to unauthorised personnel as they were secured through passwords.

Overall Summary: Conclusions for Security Risks

The study concludes that the hospital's records were at risk due to access to current and semi current records by unauthorised members of staff. The study also concludes that the non-current records of the hospital were facing no risks associated with unauthorised access to records

Summary of Findings for Storage Risks

Risk	Is the Hospital Affected by this Risk (YES/NO)	Respondents identifying the Risk	Likelihood of Risk Affecting the Hospital
Records Storage Areas in Close Proximity to Building Works	NO	0 (0%) affected	Low
Leaking Water Pipes	NO	0 (0%) affected	low
Faulty Electrical Wiring	NO YES	2 (67%) Not affected 1 (33%) Affected	Low Medium
Keeping Records on the Floor	NO	0 (0%) affected	Low
Records Areas Considered as Dumping Ground for all Kinds of Material	YES	3 (100%) affected	High

Findings: Storage

Records have to be stored in secure areas which do not have chemicals and substances which might react with records and or even spill on records. It is therefore essential that records be kept away from building works. All the 3 respondents highlighted that their records storage areas were not in close proximity with building works. However, all the 3 respondents highlighted that their records were kept in close proximity to kitchens and toilets. All the 3 respondents also highlighted that records were being stored in close proximity to hospital laboratories and workshops.

The 3 respondents however, highlighted that there had been no cases of leaking water pipes that had affected records storage areas and records. Records storage areas must also not have faulty electrical wiring as such may cause fires within a records storage area. Records storage areas must not have bare and sagging electrical lines. However, 2 of the respondents highlighted that their records storage areas had faulty wiring and damaged equipment.

It is also risky to store records on the floor as water pipe leaks might destroy the records. However, in some organisations records are stored on floors owing to the shortage of storage space. The 3 respondents in this study highlighted that they were not storing records on floors

in their respective units. However, all the 3 respondents highlighted that records storage areas were being considered as dumping grounds for all types of material and equipment. The data also showed that there were no unstable record formats such as combustible nitrate film stored in the records storage areas.

Summary Conclusions for Storage Risks

This study concluded that the major risks to records in storage areas was that hospitals records areas were considered as dumping ground for all kinds of material, whereas the risk posed by faulty electrical wiring was also noted. On a positive note, it emerged that there were no cases of leaking water pipes, neither were there cases of records storage areas in close proximity to building works.

Summary of Findings: Implementation of Disaster Planning

Risk	Is the Hospital Affected by this Risk (YES/NO)	Respondents identifying the Risk	Likelihood of Risk Affecting the Hospital
Absence of Records Risk Priority List	YES	3 (100%)	High
Absence of Disaster Response Plan	YES	3 (100%)	High
Absence of Business Continuity Plan	YES	3 (100%)	High

Findings: Implementation of Disaster Planning

It is essential that organisations, hospitals included, to have disaster preparedness and records recovery priority lists. Such will come in handy when disaster strikes and such plans be used to show which records are of importance and must be prioritised when recovering records. This is because organisations may go at lengths in protecting records whose importance is less whilst not recovering vital records. However, this assessment established that the hospital did not have a records recovery priority list. The data also showed that the hospital did not have disaster response procedures and records recovery priority lists. The data also showed that there was no business continuity plan in the hospital. Disaster response plan and the

absence of a business continuity. Without such documents and plans, the hospital was susceptible to failure to salvage records and even survive any possible disasters,

Recommendations

This study recommended that the hospital must draft a disaster response plan, business continuity plan and records recovery priority list. The presence of such documents will help the hospital prioritise on what to be salvaged in cases of disaster and avoid failure to salvage the most important and vital records. Furthermore, there has to be a strategy for business continuity as the hospital has to continue operating even after the disaster.

The study also recommended that security measures be put in place to avoid unauthorised personnel from accessing records. The researchers further recommended that faulty electrical wiring in records storage rooms be fixed and that the records storage rooms be not used as dumping grounds for all kinds of material. The researchers also recommended that air conditioners be purchased in order to keep temperatures in records storage areas stable. Furthermore, the researchers recommended that dimmers be used in records rooms being affected by sunlight as this will lead to the deterioration of records.

Reference

Canadian Medical Protective Association. 2014. *Electronic records handbook*. Canadian Medical Protective Association.

Chaterera, F. 2016. Managing public records in Zimbabwe: the road to good governance, accountability, transparency and effective service delivery. *Journal of the South African Society of Archivists*. 49:116:136

Daly, R. 2015. Poll: *One-Fifth of Hospital EHRs Are Poor Fits: Switching may be necessary for some hospitals to meet federal incentive program requirements and avoid upcoming Medicare penalties*.

Doherty, D. and Carino, R. 2015. Critical risks facing the healthcare industry. Philadelphia: ACE Group.

Emery, P. nd. *Why records management*. Recall Corporation.

Health Practitioners Council of South Africa. 2006. *Guidelines for good practice in the healthcare professions: Guidelines on the keeping of patient records*. Health Practitioners Council of South Africa: Pretoria.

Irish Standard ISO 31000:2009 Risk management – Principles and guidelines

Kalusopa, T. 2011. *Developing an e-records readiness framework for labour organisations in Botswana*. Doctor of Literature and Philosophy: University of South Africa.

Lihoma, P. 2012. The impact of administrative change on record keeping in Malawi. PhD thesis.

Ndenje-Sichalwe, 2010. *The significance of records management to fostering accountability in the public sector reform programme of Tanzania*. PhD Thesis: University of Kwazulu Natal.

Mangalmurti S. S., Murtagh, L. and Mello, M. M. 2010. Medical malpractice liability in the age of electronic health records. *New England Journal of Medicine*, 363: 2060-2067.

Ministry of Health and Child Welfare, Zimbabwe. 2012. Zimbabwe's Draft E-health Strategy 2012-2017. (Online). Available at:

http://www.who.int/goe/policies/countries/zwe_ehealth.pdf (Accessed 20 June 2016).

Medical Insurance Exchange of California. 2008. *Medical record documentation for patient safety and physician defensibility: A Handbook for Physicians and Medical Office Staff*. California, Oakland, CA.

Medical Protection Society of South Africa. 2014. *Medical records in South Africa*. Medical Protection Society of South Africa: Pretoria.

National Archives, Britain. 2010. *Guide 2: Organisational arrangements to support records management*. (Online) Available:

www.justice.gov.uk/guidance/docs/foi-section-46-code-of-practice.pdf (Accessed 12 June 2016)

Office of the National for Health Information Technology (USA). 2015. Guide to privacy and security of electronic health information. (Online) Available:

Penn, I., Pennix, G. and Coulson, J. 1994. *Records management handbook*. 2nd ed. Aldershot: Gower.

Poba-Nzaou P. Electronic Health Record in Hospitals: A Theoretical Framework for Collaborative Lifecycle Risk Management. *Journal of Healthcare Communication*, 2016, 1:2.

Queensland State Archives. 2010. Digital Archiving Discussion Paper: Informing an approach to the long-term management and preservation of government digital records. (Online). Available at:

<http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/QSA-DigitalArchiving-Discussion-Paper.pdf> (Accessed 22 June 2016).

Royal Cornwall Hospitals Trust. 2011. *Records management strategy*. Royal Cornwall Hospitals Trust.

Wold, G. H. and Shriver, R. F. 1997. Risk analysis techniques: the risk analysis process provides the foundation for the entire recovery planning effort. *Disaster Recovery Journal*. (Online) Available:

http://www.drj.com/new2dr/w3_030.html (Accessed 20 June 2016).