ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Framework for Enhancing e-Health Security: Case of South African Healthcare

Phathutshedzo Nemutanzhela

PhD Student, Dept. of Informatics, Namibia University of Technology, Windhoek, Namibia

ABSTRACT: Many of the major forces of change impacting healthcare today have technological underpinnings, and many of the less desirable impacts may have technological solutions. Two related technological forces are transacting business, online (e-business) and delivering healthcare online (e-Health)."

The movement to improve the quality of healthcare does not lack established interventions, powerful ideas, and examples of success and breakthrough results. Uptakes of these advances, however, are limited, uneven, and slow. As a result, many patients receive less than basic care, thereby increasing the risk of negative outcomes for both patients and providers. A major challenge for global health systems is to spread these advances broadly and rapidly, adapting them for different care settings. Some Benefits of Information and Communication Technology (ICT) in healthcare delivery are that advanced information technologies furnish healthcare providers with the opportunity to improve patient care by streamlining clinical processes and creating a seamless flow of information in addition to containing costs.

Currently, healthcare providers use e-Health records to record a patient's receipt of healthcare services. Unfortunately, security is still a major issue that need enhancement in order to deliver a best and secure services to all the patients.

KEYWORDS: Information and communication Technology (ICT),e-Health, Security, Privacy, Contingency Theory

I. INTRODUCTION

In relation to healthcare institutions hospitals, company requirements relate to staffing, workflow and business development. Environmental conditions comprise such factors like regulation and set of laws, accreditation/certification standards and refund from third-party payers and rivalry from other healthcare providers. From a contingency theory standpoint, information systems may serve to fill company requirement and/or to deal with environmental prospect or threats, with decisions about information system implementation being made in the framework of organizational resources and approach so to accomplish a "good fit."

Contingency theory, particularly, is playing a crucial role in information science theory [1]. Sharma and Yetton [2]example, appeal to a contingency framework to give details to the effect of user training on implementation of information systems. In the same way, Hutzschenreuter and Listner [3] expand a contingency theory model for knowledge management and sharing, and [4] look at the influence of data processing on goal contingency. [5] look at the contingency theory framework to explore the influence of exogenous contingent factors on decisions to apply strategic information systems.

Contingency theory supports that an enhanced link between organisation and structure has affirmative effect on performance that forecast positive results. Where the structure does not fit well with the organisation, the outcomes are minimal. Contingency speak to the relationship between fit and performance [6]. Fit performance is the most common element of contingency theory.

According to [7] the main purpose of fit is to improve the company's social performance. When contingency theory is applied, considering how people involved in a healthcare institution sees the situation, can assist in establishing which approach could be best to the stakeholder – organisation relationship and restore the company reputation

II. RELATED WORK

Information and Communication Technology

Information and communication technologies have changed the face of the world we live in. ICT enables people to communicate with family, friends and colleagues around the world instantaneously, gain access to global libraries, information resources, and numerous other opportunities. ICT may also bring an improvement in healthcare delivery systems [8].

According to Institute of Medicine, [9] the application of information and communications technology (ICT) in health care has grown exponentially over the last 15 years and its potential to improve effectiveness and efficiency has been recognized by governments worldwide.

Security

There are many characterizations of computer security. The one we use is related to the term information technology security. Information technology security is defined in a document [ITSE91] created by the European Community, which has gained some recent international acceptance [10].
The document [ITSE91] defines information technology (IT) security to include the following:

- Confidentiality. Prevention of unauthorized disclosure of information.
- Integrity. Prevention of unauthorized modification of information.
- Availability. Prevention of unauthorized withholding of information or resources.

The concept of privacy is a fundamental motivator for security. Privacy is commonly understood as the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. By extension, privacy is also associated with certain technical means (e.g. cryptography) to ensure that this information is not disclosed to anyone other than the intended parties, so that only the explicitly authorized parties can interpret the content exchanged among them.

Data integrity is the property that data have not been altered in an unauthorized manner. By extension, data integrity also ensures that information is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

Through information systems, an organisation executes its business strategy and attempts to realize its business goals. Lederer and Gardiner [11] refer to this as ‘a portfolio of computer-based applications’. Many organisations use IS as tool for their various innovations to support and enable processes and activities.

E-health

E-health is a relatively new term in healthcare practice and one of the most rapidly growing areas in health and ICT today. The World Health Organization defines e-health as the cost-effective and secure use of information and communications technologies (ICT) in support of health and health- related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research. WHO,[12] “e-Health is the use of information and communication technologies for health”

E-health is defined as the application of Internet and other related technologies in the healthcare industry to improve the access, efficiency, effectiveness, and quality of clinical and business processes utilized by healthcare organizations, practitioners, patients, and consumers in an effort to improve the health status of patients [13].
“E-Health describes the application of information and communications technologies (ICT) across the whole range of functions that help health. It is the means to deliver responsive healthcare tailored to the needs of the citizen [14].”

III. METHODOLOGY

The case study method was selected mainly for the following reasons; the case study method provides detailed information and it’s holistic in approach. According to [15], ‘The case study method is useful when detailed knowledge is required of any particular case'. The case study method provides opportunity to create new hypotheses and also create an interest for further study in the field of information systems. This is supported by [16] who argued that 'a single, well-designed case study can provide a source of new hypotheses and constructs simultaneously'.

Organisations that are strong in Adaptability and Involvement have an edge in innovation and creativity, while organisations excelling in Mission and Consistency have a high measure of stability, return on investment and return on sales. Organisations measuring high in all components have a dramatic financial advantage over organisations that are weak in these areas. Organisations at the bottom perform just as one would expect: They are sluggish, wasteful and out of touch with their customers [17].

Therefore, the study has adopted contingency theory because it covers prevention, detection and reaction to threats, vulnerabilities and impacts inside and outside and organisation. This theory is to recognize and respond to variables in order to attain organisational objectives effectively.

Using contingency theory to address security

The essential affirmation of Contingency Theory is that the milieu in which a company operates determines the most excellent means for it to manage. For that reason, the study has adopted Contingency Theory for the reason that it includes how to prevent, detect and react to threats, weaknesses and impacts in and out of an organisation. This theory is to distinguish and act in response to variables including confidentiality, privacy, Integrity and security of data so to accomplish the goals of the organisation successfully.

IV. DATA ANALYSIS

This section presents the analysis from two Healthcare institutions HC1 and HC2 and also with supporting data that was collected from one of the two healthcare rendering same services, HC1 is a more advance than HC2 as all the e-health implementation starts at Healthcare 1, This analysis provides an insight on the contingency planning process and how decision processes were followed in the selection of technology and strategy used to enhance the Confidentiality, Security and Privacy of Medical Records in a rural setting. Contingency planning directly supports an organisation's goal of continued operations. These two healthcares from High Mapara Care name change because of anonymity were chosen because they have already started with the process of introducing a system that deals with electronic Medical Records.

The analysis was done at two different levels, macro and micro levels, individual and group, respectively. Each participant in the case studies was labelled as follows: in Healthcare 1, as HC1001_01 to HC1001_010 and in Healthcare 2 as HC2001_01 to HC2001_010 irrespective of whether is a patient or a healthcare practitioner.

The study is aimed at investigating and understanding the role of technology in enhancing the Confidentiality, Security and Privacy of Medical Records in a rural setting. The findings from each case are discussed in parallel using a contingency theory. According to [18] Organisations should practice contingency planning because it makes good business sense. Contingency planning addresses how to keep an organisation's critical functions operating in the event of disruptions, both large and small. This broad perspective on contingency planning is based on the distribution of computer support throughout an organisation.

The following six steps describe the basic functions an organisation were employed when developing contingency plans. The interpretations to get to the findings of the study were applied using three factors of Contingency security model [19] which is processes, people and technology.

Processes

The human factor not only plays a pivotal role in the confidentiality, privacy and security of e-health services for users. It is also an extremely important issue for the service providers themselves. For this reason, providers should operate a dedicated information security management system (ISMS) which defines processes and rules for the effective management of information security. ICT providers in the healthcare must also draw up rules that ensure employees meet security requirements and specify which users can access which systems and data and who is responsible for which operational and security-related tasks.

According to one employees HC1001_03 (p4:30-31); Privacy and *security of patients record depends on how you value your work, whether we have system that encrypt patients record or a paperless system, if as an employee I don't respect the security of patients records , or don't know what it means to know other people health status. Then I will end up telling friends and family without realising the damage I am making to the image of my patients and his confidence. However, one of the patient HC1001_03a, state that "when I go to see a healthcare practitioner, I believe that all my records are secured. I tend to feel at ease.*

The scope and type of ICT services must be defined in a written agreement. Requirements must be outlined and any necessary changes need to be implemented and monitored. Organisational structures and processes must be in place to enable a rapid response to security incidents or threats. Services must be clearly defined in a service level agreement (SLA), and mission critical applications need to be identified to ensure the correct levels of availability and security. Documents should also outline emergency procedures, including the sequence in which systems will be reactivated following failure or downtime. According to one the interviewees HC2001_010 (p13:100-103), "*Users must comply with legal, regulatory and industry-specific requirements, including in-house policies, contracts with customers, suppliers and partners, and other obligations. Users need to verify that their cloud service provider can meet these imperatives. Data protection legislation varies widely from country to country. Organisations also differ in terms of processes and potential threats, and the extent to which security incidents would negatively impact the business*".

People

Identity management, including roles and rights, end-point security and access control, is a cornerstone of any ICT security solution, but is particularly important when it comes to the cloud. If employees can access business critical information, there is always a risk that this will be misused, and if outside persons can access this information the danger is even greater. Thus applying stringent identity management, security and access control on a need-to-know basis is a vital foundation component of an end-to end cloud security solution. Therefore HC1001_011 (p11:102-104) started that, "*Exploring patient expectations is very important for ensuring healthcare is highly secured. There is a magical increase in the expectations of the patients and a wide gap exists between patient expectations and general practitioner perceptions of medical care. Therefore, to ensure good general practitioner care, a satisfactory balance should be achieved between patient expectations, general practitioner perceptions and priorities set by healthcare planners*". She further expressed that, "*if employees can learn how to take cognition of the security guide lines and use the system provided by healthcare to capture patient records, this can reduce patients worries as all patients information will be on a secured system rather than a paper that most people can access. All security processes to be followed must be documented and made available to all concern parties*".

The World Health Organization (WHO) recently noted that countries, particularly those in Africa, will not develop economicallyand socially without substantial improvements in the health of their people. According to one of the physician HC2001_06 (p7:98-100) started that "*Keeping in mind that the ultimate goal of e-Health should be to strengthen health systems and improve people's health. Patients share a basic understanding of security of records, but some might have expectations that are likely not met by current practice nor anticipated by doctors. Therefore, doctors should recognize that patients might have their own model on how to secure healthcare record. They should address divergences from current practice and provide support to those who face emotional or practical obstacles to self-revelation*".
Sharing of this knowledge becomes a challenge. According to HC1001_04 (p4: 45-48) started that "*this will include identifying people in resource-poor countries who can provide mentoring and basic education in informatics; expert consultation that enables decision makers to make wise policy choices; and acquisition of informatics tools.*"

Technology

With e-Health services it is essential that data not be compromised when transferring between the user and the service provider. When data is sent over public networks such as the Internet, it must be encrypted to prevent access by unauthorised parties, to safeguard integrity and confidentiality. Secure remote access should be enabled using a Virtual Private Network (VPN) or cryptography. HC1001_011 (p25:283-284) emphasized this fact, even further, when he said that *the human intervention is the most important determinant of the organisation's survival and growth. Humans, thus, determine which assets to apply or not to apply and, consequently, when to act or not to act. This drives a privacy and* *security force; in particular that of our management cadre, as well as the group dynamics of such a management team, because they always have a prominent influence on determining how such a private and secure force will approach the possible opportunities, uncertainties and threats of the future business environment. Knowledge of such a human is what adds a new dimension to determining the future intent of a private and secure force, and enables the organisation to make right decisions.*

Managers and users of IT systems must select among various standards when deciding to use cryptography. Their selection should be based on cost-effectiveness analysis, trends in the standard's acceptance, and interoperability requirements. In addition, each standard should be carefully analysed to determine if it is applicable to the organization and the desired application. As patients' expectations rise, patient care becomes more complex, and resources continue to shrink, hospitals are finding that traditional approaches to defining, organizing, and staffing confidentiality assurance functions are no longer adequate. According to HC1001_10 (p13:111-113) expressed that "*More and more, hospitals are becoming convinced that improving confidentiality requires a broad, whole-hospital consensus about what confidentiality means, who is responsible for it, and how key hospital groups should communicate with one another about confidentiality issues*".
However, HC1001_02(p3:33-36) "The reason for building security of healthcare records into health Information Technology (IT) systems was initiated to bolster trust in such systems and promote their adoption". He then further explained that "Security issues, too long seen as a barrier to electronic health information exchange and this can be resolved through a comprehensive model that implements core security principles, adopts trusted network design characteristics, and establishes oversight and accountability mechanisms".

Although it is impossible to think of all the things that can go wrong, an organisation should identify a likely range of problems. Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as study, can point to other possible, but less obvious, contingencies. According to one of employees, HC1001_06(p10:90-94) "*The need to integrate decision support systems to become one of paperless healthcare system for security of healthcare records is recognized as an important objective in building patient trust necessary for successful health outcomes. Little is known about patient understanding and expectations of the security of healthcare.*

However, HC2001_04(p10:50-54) because this healthcare organisation has been using different systems, that all of them do different things and they don't even communicate to each other, therefore the challenges of implementing or integrating this system is complex and will take long to actually function completely even though it's vital to, integrate the systems to develop security rules for personal health records, a more nuanced approach to the role of consent, and stronger oversight, accountability, and enforcement mechanisms. The challenge is to find the right mix of statutory direction, regulatory implementation, and industry best practices to build trust in e-health systems and enable the widespread adoption of health IT.

According to HC1001_03 (p5:76-80) said that "Security is the expectation that something done or said would be kept "secured" but differed on what information was secure and the basis and methods for protecting information". However she also said that "Some consider all medical information as secure and thought security of data functioned to limit its circulation to medical uses and reimbursement needs. Others defined only sensitive or potentially stigmatizing information as secure". Security of healthcare is a strict limit prohibiting information release, although some noted that specific permission or urgent need could override this limit.

V. FINDINGS

From the analyses and findings, the two cases studies provide insight to the different characteristics in the field Security of healthcare Medical Records.
A framework was developed. This Framework (Figure 1) integrated framework for enhancing e-Health Securityis aimed at framework for Enhancing e-Health Security. Security was identifying as a major concern that if addressed the other two aspects (confidentiality and privacy) will also be addressed.
To have a full understanding of this framework a discussions that follows should be read with the figure:

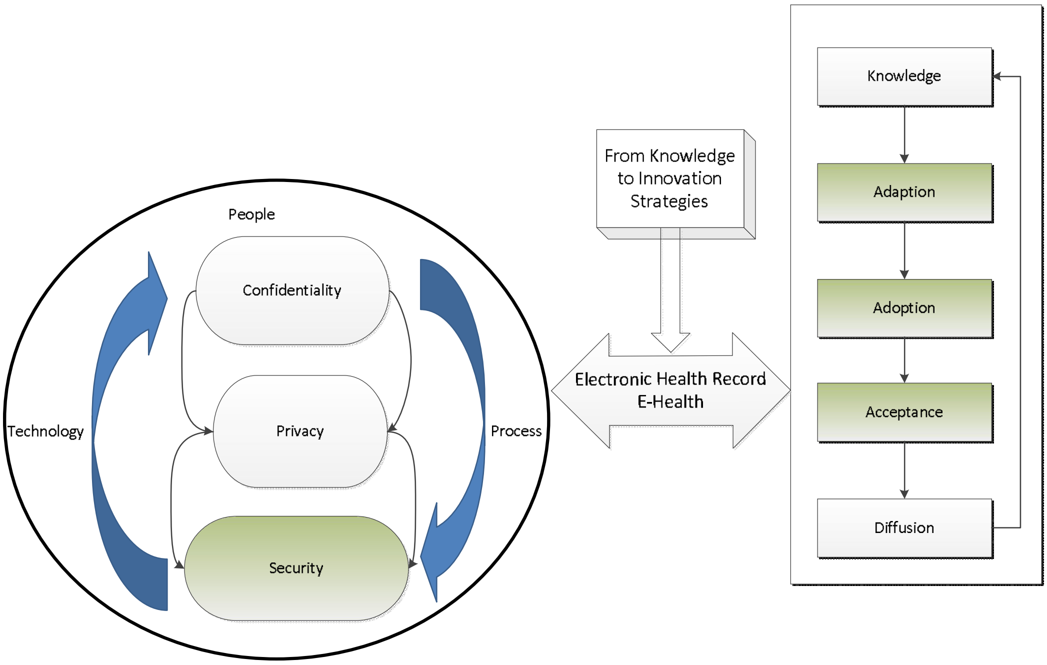

Fig.1. Integrated framework for enhancing e-Health Security

Healthcare that are strong in technology and Policies drafting have a drive in security of Medical Records, while organisations excelling in Mission and Consistency have a high measure of stability, integrity and clients trust. One of the foremost of these is the privacy issues raised by adapting electronic storage and communication, due to the sensitive nature of health data. Indeed, privacy in e-Health has been recognised as one of the paramount requirements necessary for adoption by the general public Survival of an organisation is based on how secure is the system or technology that they are using. Policies become a baseline of each healthcare, for Medical Records to be secure and have confidential it requires a proper implementation of policies. That requires the healthcare people to accept changes and rules to follow with regards to security.

Healthcare measuring high in all components have a competitive advantage over healthcare's that are weak in these areas. Healthcare's at the bottom perform just as one would expect: They are sluggish, wasteful and out of touch with their customers.

Administrators in healthcare delivery organisations have to be mindful that adoption of knowledge management practices would be dependent on leadership, Information Technology(IT) Infrastructure (and integration) and supporting policies in human resource management. As physicians within healthcare delivery organisations normally gain experience through a mentor-apprentice route, an organisational culture that promotes and rewards such behaviour would be beneficial.

A differentiated corporate policies and technology can build sustainable long-term competitive advantage and help to attract and retain talented staff. Policies must be ideal as to what are business rules and procedures when it comes to security, confidentiality and privacy of patients records. All aspects of the business security, privacy and confidentiality of electronic Medical Records must be addressed during a policy drafting planning.

People are the most important tools of the whole process as they are involved in strategic planning. They are the ones who utilise the technology in questions. Patients also form part of people. Therefore, people are the driver of the business and decision makers.

After a technology has been chosen and strategy has been drawn, organisations have to decide on current. This drives security force; in particular that of our management cadre, as well as the group dynamics of such a management team, because they always have a prominent influence on determining how such a private and secure force will approach the possible opportunities, uncertainties and threats of the future business environment. Knowledge of such a human is what adds a new dimension to determining the future intent of a private and secure force, and enables the organisations to make right decisions.

Policies and process need to be followed carefully when addressing issues related to security of data. If the policies and processes are addressed properly it is easy to draw a good structure of how to tackle these issues. They see the most pressing need as developing a structured and systematic approach to what is known as knowledge sharing. People like to share information regardless of how confidential it is, that's why policies and process with regards to Confidentiality, Security and Privacy of Medical Records need to be addressed. Security has gained increasing attention in recent years and has become more relevant in the fast changing, IT-driven world; primarily due to the fact that organisations always want to stay ahead of their competitors.

Prescribed stage is a loop because an organisation should test and revise the contingency plan. A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and its implementation.
Contributions: Our main contribution is to identify two new types of enforcing privacy as key privacy challenges for the field: enforced privacy (e.g., a doctor cannot prove to a pharmaceutical company which medicine he prescribed) and privacy in the presence of others (e.g., a patient cannot reveal which doctor prescribed her medicine). We propose to use formal techniques to address these challenges, that is: to understand and interpret these new privacy notions in a precise and unambiguous manner, and to build an efficient verification framework for analysing privacy properties of e-Health systems.

The term contingency as used in contingency theory is similar to its use in direct practice. A contingency is a relationship between two phenomena. If one phenomenon exists, then a conclusion can be drawn about another phenomenon. For example, if a job is highly structured, then a person with a freewheeling disposition will have problems with the job. Contingencies can sometimes be considered conditions. Hence, we analysis this study and come with arrears that are affected by Confidentiality, Security and Privacy in the healthcare
Healthcare delivery also presents a very a unique situation exists where the primary loyalty of the professionals belong to their profession rather than to the organisation.

Furthermore, healthcare delivery is moving away from a physician-patient relationship to a customer-company relationship, and at the same time the traditional single physician-patient relationship is moving towards a situation where the healthcare is delivered by a team of healthcare professionals where in each specialize in a single aspect of healthcare.

Diffusion of knowledge in organisations is multidimensional, and can be understood across functional lines such as financial, human resources, organisational learning etc. Diffusion of knowledge in healthcare delivery can be studied along the different domain of activities, and across the dimensions of effectiveness, accessibility and efficiency.

Quality of healthcare and patient care can be viewed both in terms of outcome and the degree to which the need and expectation of the patient has been meet in terms of technical and interpersonal care.

VI. CONCLUSION

It is important to bear in mind the full lifecycle of technical and standardization activities: business need, development, adoption, adaptation or localisation, accreditation and standardisation. These aspects all need to work together as a system to build trust. However this needs all stakeholders to be fully and actively engaged. There are four viewpoints that need to be reconciled: healthcare users, who need IT support which is understandable, affordable and adoptable; suppliers, who make money by delivering value; policy leads, whose main perspective is the improvement in health; and patients and citizens.

Ideally, each of these will be able to contribute to developments and see their needs fulfilled. An important part of the recommendations is to enable this dialogue to be successful. The following are seen as critical success criteria for standardisation activities, building on current initiatives and best practice:
Relevance: Those standardisation activities are seen as relevant to business objectives and current activities;

° Openness: that standardisation is seen as an open and inclusive process which removes rather than presents barriers for progress;

° Engagement: that all parties are able to contribute, from prioritization of business requirements through development, implementation and maintenance;

° Affordability: that resulting standards are affordable, and demonstrating a clear return on investment.

° Sustainability: that the framework for development of interoperability standards is sufficiently open and flexible to allow continues adaption and development as the solutions and market evolve.

The aim is that successful completion of the recommendations will ensure these criteria are met.

REFERENCES

1. Weill P. and Olson M.H. “Managing Investment in Information Technology: Mini Case Examples and Implications”, MISQ, March 1989.
2. Sharma, R and Yetton, P. “The Contingent Effects of Training, Technical Complexity, andTask Interdependence on Successful Information Systems Implementation”, MIS Quarterly, 31 (2), pp.219– 238, 2007.
3. Thomsen, J., Levitt, R.E., & Nass, C.I. “The virtual team alliance (VTA): ExtendingGalbraith’s information-processing model to account for goal in congruency”. Computational& Mathematical Organization Theory, 10(4): 349-372, 2005.
4. Hutzschenreuter, T., & Listner, F. “A contingency view on knowledge transfer:Empirical evidence from the software industry”. Knowledge Management Researchand Practice, 5(2): 136-150, 2007.
5. Silva, L., and Hirschheim, R. “Fighting Against Windmills: Strategic Information Systems and Organizational Deep Structures,” MIS Quarterly (31:2), pp. 327-354, 2007.
6. Donaldson, L., Sage, Thousand Oaks.Eccles, R.G., and Nohria N. The Contingency Theory of Organizations beyond the Hype: Rediscovering the Essence of Management, Harvard Business School Press, Boston. 2001.
7. Husted, B. W. “A Contingency Theory of Corporate Social Performance”, Business and Society, Vol. 39 No. 1, pp. 24-48, 2000.
8. Idowu, B., Ogunbodede, E., Idowu, B. “Information and Communication Technology inNigeria: The health sector experience”. Journal of Information Technology Impact, 3(2), 69-76, 2003.
9. Institute of Medicine, authors. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC: National Academies Press; 1 Jun 2001. http://www.nap.edu/books/0309072808/html
10. Donald L. Brinkley and Roger R. Schell.Concepts and Terminology forComputer Security. Essay 2. Accessed [20 November 2014]http://www.acsa-admin.org/secshelf/book001/02.pdf
11. Lederer, A.L & Gardiner, V. “The Process of Strategic Information Planning", Journal of Strategic Information Systems, 1 (2): 76 – 83, 1992.
12. WHO. Health and the Millennium Development Goals. Geneva: WHO http://www.who.int/mdg/publications/mdg_report/en/index.html. 2005.
13. Silber D. Silber D. The case for eHealth. (Presented at the European Commission’s first high-level conference on eHealth .European Institute of Public Administration, May 2003.
14. Marconi, J. “E-Health: Navigating the Internet for Health Information Healthcare”, Advocacy White Paper. Healthcare Information and Management Systems Society, May 2002.
15. Hofstee, E. Constructing a Good Dissertation: A Practical Guide to Finishing a Master's, MBA or PhD on schedule, EPE Publishers, Sandton, South Africa. 2006.
16. Cooper, D. & Schindler, P. Business Research Methods, McGraw-Hill/ Irwin Series, New York. 2006.
17. Nemutanzhela, P and Iyamu, T. “A Framework for Enhancing the Information Systems Innovation: Using Competitive Intelligence” The Electronic Journal Information Systems Evaluation available online at www.ejise.com.Volume 14 Issue 2, (pp242-253), 2011.
18. Scott, W. R. Organizations: Rational, Natural, Open. Englewood Cliffs, N.J.: Prentice-Hall. 1992.
19. Daniel E. O’Leary. “Enterprise Resources Planning (ERP) Systems: An Empirical Analysis of Benefits” journal of emerging technologies in accounting Vol. 1, pp. 63ñ72, 2004.

BIOGRAPHY

Phathutshedzo Nemutanzhelais a Part Time Lecture in the Information Technology (Informatics) Department, Tshwane University of Technology (TUT), South Africa. She received Master of Business Information System (BIS) degree in 2010 from TUT. Currently enrolled for a PhD degree in Informatics. Her research interests are Competitive Intelligence, Information System, Innovation, Mobile Health or E-Health.