A ROLE-BASED SECURITY AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

Ophola Maseti[a], Dalenca Pottas[b]

a Department of Information Technology, Nelson Mandela Metropolitan University

b Department of Applied Informatics, Nelson Mandela Metropolitan University

[a] Opholo.Maseti@nmmu.ac.za, +27 82 6766910, PO Box 77000, Port Elizabeth, 6031

[b] Dalenca.Pottas@nmmu.ac.za, +27 41 5049100, PO Box 77000, Port Elizabeth, 6031

ABSTRACT

The use of electronic systems to access information is advancing rapidly. Many aspects have to be considered in regards to such high availability of information, for example, training people how to access and protect information, motivating them to use the information extensively, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. This is especially true in the health sector, where access to critical data is often vital. This data must be accessed by different kinds of people with different levels of access.

However, accessibility often leads to vulnerabilities. The health sector deals with very sensitive data. People's medical records need to be kept confidential; hence, security is very important.

This paper firstly provides an overview of how South Africa is doing compared to the rest of the world as regards to central accessibility of health information as well as the level of technology adoption. A brief investigation of security and privacy-related issues which hinge on the central accessibility of this data is reported on. A model is developed which can be used to create a security awareness checklist. Such a checklist constitutes a self-assessment tool for care-givers in the South African health sector, to gauge awareness in regards of information security and privacy.

KEY WORDS

Health Sector, Health Information Systems, Security and Privacy, Security Awareness

A ROLE-BASED SECURITY AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

1 INTRODUCTION

The success of both the public and the private the health care system being dependent on the ability to consolidate information from a variety of sources has been reached as the general consensus in the South African health care environment (Committee on Standardization of Data and Billing Practices, 2003).

The use of electronic systems to access information is advancing rapidly. Many aspects have to be considered in regards to such high availability of information, for example, training people how to access and protect information, motivating them to use the information extensively, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. This is especially true in the health sector, where access to critical data is often vital. This data must be accessed by different kinds of people with different levels of access.

However, accessibility often leads to vulnerabilities. The health sector deals with very sensitive data. People's medical records need to be kept confidential; hence, security is very important.

It is always necessary for information to be accessible especially in the health sector. Such accessibility (or availability) is further augmented in an integrated environment. For example, a Health Information System (HIS) may be linked to laboratory systems that give the results of certain tests on patients, to emerge with specific data. This data must then be transferred to the patients' medical records automatically without human intervention.

In South Africa, the use of electronic systems in the health sector to share patient information has been slow. The initial plan was to form the National Health Care Management Information System partially by the public and private sector. The formation of this system would ensure proper management of hospitals as well as the key functions and service requirements of the health sector. Thus far, the implementation of this system has not been successful as it is not available in all provinces.

Regardless of the level of integration and / or technology adoption, the fact remains that information of a very sensitive nature, is exposed to human intervention on various levels (e.g. nurses, administrative staff, general practitioners and specialists). In this scenario, it is important for each person to be aware of the requirements in terms of security and privacy, especially from a legal perspective.

This paper firstly provides an overview of how South Africa is doing compared to the rest of the world as regards to central accessibility of health information as well as the level of technology adoption. A brief investigation of security and privacy-related issues which hinge on the central accessibility of this data is reported on. A model is developed which can be used to create a security awareness checklist. Such a checklist constitutes a self-assessment tool for care-givers in the South African health sector, to gauge awareness in regards of information security and privacy.

2 THE HEALTH SECTOR: TRANSFORMATION AND TECHNOLOGY ADOPTION

2.1 Reform of the South African Health Sector

South Africa has had an unfortunate event of the apartheid in the past. Back then, there were too m any policies from the apartheid government that were not allowing all South Africans access to proper health care. Now that South Africa is a free and democratic country, all the damage from the

past would need to be unravelled by the government. All legislation, organisations and institutions related to health had to be reviewed with the involvement of the complete transformation of the national health care delivery system (ANC, 1994a).

"When we started the term of office of this government in 2004 we set ourselves a series of goals which we sought to achieve when this term ends in 2009. These goals are contained in a document which we called "Strategic Priorities for the Health Sector 2004-2009 (popularly called the 10 Point Plan)"" (Department of Health, 2006, Online). It clearly shows that the government is aware that the health sector needs to have serious changes to be effective, towards the benefit of all South Africans. The Department, as is reflected in the Plan will improve the health facilities and the quality of care that is provided in these facilities, both clinics and hospitals. In this regard they plan to introduce a hospital improvement plan in April 2006. With respect to health programmes, two programmes have been prioritised in line with the decisions taken by World Health Organization, Regional Office for Africa (WHO/AFRO). During 2006 a TB Crisis Plan will be launched to deal more decisively with the burden of disease from TB as well as an Accelerated HIV Prevention Plan (Department of Health, 2006, Online). The government must have some means to measure their achievements against their goals.

In order to know your progress in terms of achieving your goals, it is imperative that you reflect on what you were able to achieve thus far. "These priorities are based on an assessment of what we have achieved in the past 10 years and what work remains to truly transform the health system to better meet the needs of all those who live in South Africa. Whilst we are justifiably proud of our achievements we need, in the next five years to work hard with our partners to strengthen the health system so that we can provide accessible, good quality health services to all" (Department of Health, 2004, Online). The government is willing to compromise and work very hard with its partners and bring fresh ideas that would ensure that the health system of South Africa is strengthened. This is good news for the South African public, as the government has had problems with ensuring that delivery in the Department of Health is of good quality.

The District Health Information System, despite persistent problems with data quality, data flows and utilisation of data/information has been a major achievement and largely a unifying force across the country (Hedberg, 2003, Online). The Department of Health further adopted a National Policy on Quality in 2001 (Department of Health, 2004, Online). Based on the national policy, all the provinces have now established provincial policies and quality assurance units to lead and co-ordinate efforts on quality improvement, there are also complaints systems and procedures in place for all the provinces and the national department. To support this notion even more, the government has to ensure that there is proper infrastructure and resources throughout the whole country. This can be done by investing and spending money wisely in the health sector.

Calle Hedberg (2003), who is a Researcher and a Systems Designer at the Health Information Systems Programme claims that the Government expenditure on Health Care Information Systems has not changed in line with the shift towards the Primary Health Care approach (Hedberg, 2003, Online). The author alleges that 90 to 95% is spent on advanced Hospital Information Systems in larger hospitals, which is believed to be why the South African health sector has a slow improvement in technology. The South African government has been spending a small amount of money in making sure that good health care is affordable for all South Africans. South Africa spends R550 per person per year on health care which is only 5% of GDP (ANC, 1994b, online). The World Bank estimates that ten times more should be spend to provide basic health care for all. To date, around 2004, this GDP value has gone up to 8.5% (Department of Health, n.d., Online). In order to ensure that South Africa does really reach its true potential with regards to the reformation of the health sector, there must be proper planning and corruption should be prevented by all means.

It must be derived from the fact that the state is the largest social institution, therefore its capital, human resources, managerial, technological and organisational requirements must be expected to reflect the society from which it originates (Mbeki, 2005). The Government is surely

paying attention with regards to the reformation of the health sector in South Africa. The Government has got a good plan from a strategic level but the implementation of the strategy at the lowest level has not been successful because of certain factors. Amongst these factors, shortage of staff members and inappropriate infrastructure can be included but not limited to them.

Usually organisations have excellent strategies, but the mistake that they make is not communicating these strategies to the people that generate the value of the organisations (National Department of Health, 2005, Online). The document released by the National Department of Health in 2005 says that if this can be applied to the Department of Health it will mean that the front line workers and managers should be engaged in the development of these plans and the strategy of the Department of Health should be communicated to those that will assist to achieve the strategy; however, these things to be effortless in theory but they seem to be rocket science in practice. With the strategies involving technology and the health care sector involving a lot of people referred to as general practitioners, there must be a way to distinguish that whenever there is a new strategy the front line workers are included as part of that strategy.

It seems as if the Health Care Information Systems and Monitoring and evaluation is viewed as mainly a technology acquisition process aimed at purchasing a turn-key universal solution, this can cost billions of rands in the end (Hedberg, 2003, Online); it should be rather viewed as a long-term socio-cultural, political, and technical development process with short-term practical and functional applications that work. People are the ones that really make technology work. As people form part of the organisational culture, it should not be forgotten how they are going to be catered for as well as how they would be addressed whenever there is a new technology being introduced within the organisation.

2.2 Technology Adoption in South Africa

Health information technology yields huge savings as it has the potential to greatly improve health care (United States Department of Health and Human Services, 2004, Online). Since the future of health care delivery institutions lies in cost-effective health care, health care delivery institutions will need and use information technology to meet their client demands and stay competitive (Institute of Health Systems, n.d., Online). Furthermore, the author states that general purpose information technology solutions are usually insufficient for special needs of the health sector.

The South African government is under a process of enhancing the South African health sector by involving the Constitution of South Africa and the Bill of Rights. This process has to involve information technology within it. There has to be a way that this process can be measured to see if there is any progress in terms of utilising technology. Member states of the World Health Organisation (WHO) should have established “structures and processes to ensure continued improvement of the quality of health services and an appropriate development and utilization of technology”, the obligation of establishing effective procedures for the evaluation of the advantages and relevance of Health Technology both in developmental as well as routine use is also tied to this (Health Technology Assessment, n.d., Online). This subject is addressed on Goal 31 of the World Health Organisation’s “Health For All” strategy. So it is evident that the focus on the regulation and management of Health Technology is not a South African trend alone.

Both the European Union (EU) and globally (G-8) have brought forward within them health care as one of the sectors in society with great potential for Information and Communication Technology (ICT) and with great benefits to be gained through their application in the Information Society (South African Information Technology Industry Strategy Project, 2002, Online). The South African Information Technology Industry Strategy Project (2002) further states that governments must be encouraged and in particular health ministries to facilitate the implementation of what is commonly called “e-health”, international surveys reveal a huge number of public sector and industry-based studies to raise awareness of the potential of Information and Communication

Technology. With the implementation of “e-health” being emphasised at most developing countries all over the world, South Africa have hastened the concept of a District Health Information System

The District Health Information System has been implemented in all the provinces of South Africa; however the use of this data effectively has been minimal. An assessment of many hospitals in the Eastern Cape in 1999 indicated that: “Data is collected ‘at all levels in hospitals, but most of it is never used’. Indicators are submitted to the district offices, but give a ‘very bland picture of administrative activities, and no feeling of what goes on inside hospitals’. ‘Registers are non-standardized, and tend to be anarchic, and hand written’, and often on an assortment of different types of paper and books. ‘Analysis of data is minimal at all levels’.” (Shaw, 2002). If the implementation of the District Health Information is to be successful, the data collected must be analysed thoroughly and be used extensively whenever there is a need to do so. There seems to be a lack of integration between the hospitals and the district management, which is costing the advancement of the government in trying to improve the services offered by the health sector, (Hedberg, 2003, Online) professes that there have been persistent problems with data quality, but data flows and utilisation of data/information, has been a major achievement and largely a unifying force across the country. District managers must work together with the hospital managers maybe by having meetings quarterly to discuss the data that has been generated for the past three months and taking decisions thereafter that are going to benefit the public that is making use of the health services. By doing so, they would be ensuring that the utilisation of the health care data is enhanced.

In terms of data capture and use, most health districts in the country are still at level 1 (data is being captured but its quality and use requires major improvement), level 3 (data of good quality collected and used for service improvements) is the target for all health districts (Asia & Pillay, 2003, Online). The authors further say that to reach this target in all health districts, it is important that provincial, local government and district information officers work with clinic supervisors and clinic managers.

To further improve the level of health awareness by making use of technology amongst all South Africans, the Department of Health decided to develop a South African National Telemedicine System so that it could be able to offer health care services to the most distant South African rural areas. Patients who usually visit the clinics would be able to learn from the content provided by the Telemedicine System. The objective of developing this system was to narrow the gap between the poorly resourced rural areas and the urban areas. This technology promised to provide a way of sharing skills and cutting through problems caused by geographic isolation, poor transport and infrastructure as well as scarcity of skilled health professionals; this led to a Memorandum of Understanding being signed between Sentech (national signal carrier for both radio and television in South Africa) and the Department of Health in 1999 for the establishment of a Health Channel using satellite technology (National Department of Health, 2004, Online). This Telemedicine System initiative has helped to improve the level of health awareness in South Africa amongst the patients and the health care workers.

Like any employee that works for an organisation, if that employee is slotted to a role within that particular organisation, they get used to that role and become good at it. It is essential for the health care institutions to ensure that the health care professionals are able to utilise all the new technologies that the institution brings forth. A major determinant of the rate of adoption of information technology in the health care sector is the personal computing skill of health care professionals (Institute of Health Systems, n.d., Online); furthermore, if doctors, nurses and other health care professionals are comfortable with personal computing, the rate of information technology adoption in health care institutions is likely to be faster.

2.3 Technology Adoption Internationally

An explosion of health information systems with associated benefits to health and human prosperity is being witnessed, with the liberalisation of health care and telecommunications policies spreading across every continent (McDonald, n.d., Online). The author further states that "high technology" has less importance than another gigantic problem that is facing lesser developed countries, hunger.

It is alleged that in member countries of the Organisation for Economic Co-operation and Development, spending on health care is already outpacing economic growth. An understanding of larger context within which governments manage health care systems, and administrators make decisions concerning the services that will be provided must be the first thing to arise whenever any discussion about the adoption of innovations by health care systems takes place (Canadian Biotechnology Advisory Committee, 2004, Online). In America, the Institute of Medicine estimates that between 44 000 and 98 000 die each year because of lack of medical records (The White House, 2004, Online). "By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care." (Bush, 2004).

In Canada, the Commission of the Future of Health Care paid considerable attention to the issue of medical necessity and did not directly address the impact that biotechnology will have on the health care system (Commission on the Future of Health Care in Canada, 2002). The commission concluded that "the definition of what is considered medically necessary and covered under the [*Canada Health*] *Act* needs to be updated to reflect the realities of our contemporary health care system".

3 PRIVACY AND SECURITY ISSUES IN THE HEALTH SECTOR

Some of the long-standing needs and concerns in our society have been privacy, confidentiality, and security of personal health information especially to health care providers and the public (Buckovich, Rippen & Rozen, 1999). Health care providers and organisations is the legitimate need to access information to deliver quality health care, which is also important to the public. Since information technology has been proven beyond doubt as a way of living nowadays, the health sector has had no choice but to integrate information technology into most of its systems. With this shift came the urgent need to balance privacy and access and to develop guiding principles, policies, and legislation to ensure that the most valuable information to the public is protected safely from any unauthorised authorities. With the use of information technology on the rise, access to sensitive and personal information has been easy for more individuals and entities.

As the electronic medical record offers the promise of improved care and increased efficiency, introducing information technology into the health care creates new risks to privacy as well as new means to protect privacy (The Privacy and Security Working Group, 2003, Online). There are potential risks associated with automation and sharing of patients medical records and patients are well of these risks. Patients can be lead to withholding information that could be vital to their care, from their clinicians based on these concerns. In return, the value of the patients' medical records can be reduced to other clinicians treating the patient and to researchers and public health officials. This can be caused by the exclusion of sensitive information by the clinician as a result of the concerns about privacy and security.

One of the most important things for organisations in the modern era is to train its employees on the value that the organisation places on privacy of its customers' information, as well as how to implement the privacy protection of health information.

Audit trails can be implemented by large institutions with electronic health records. These audit trails can track both accesses and changes to records without degrading system performance. Audit systems can be a good tool to deter employees from accessing information they are not authorised, as they are aware that they actions are being captured by the system. Audit trails can be very effective if any incidents are reported, then investigated if someone breached against the rules.

4 A ROLE-BASED AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

4.1 General SETA Principles

The purpose of computer security awareness, training, and education is to enhance security by: improving awareness of the need to protect system resources; developing skills and knowledge so computer users can perform their jobs more securely; and building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems (National Institute of Standards and Technology, 2004, Online). When the SETA program is to be carried out, it must be known who is going to be educated about this program and what should they be taught.

NIST 800-16 (1998), in the NIST model states that the learning of the security education program is a continuum. It starts with awareness, constructs to training and then develops into education.

The three levels of the learning continuum can be portrayed as follows:

Awareness: As the learner is only the recipient of information and does not actively participate (NIST 800-16, 1998), the purpose of an awareness program is to stimulate and motivate those being trained to care about security and to remind them of important security practices (National Institute of Standards and Technology, 2004, Online). Posters and flyers are very helpful in assisting with this level of the learning continuum.

Training: Training focuses on providing the knowledge, skills, and abilities specific to an individual's role and responsibilities relative to IT systems (Federal Agency Security Practices, 2000, Online). There are usually two groups of users that are targeted for training, the general users and the advanced users or users with specialised skills.

Education: The Education level of the learning continuum integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge. Most organisations opt not to include security education as part of their awareness and training programs as it is part of employee career development.

Each person has a responsibility to every other person. All IT services are at risk when an incident happens. It is of importance that all the role players in an organisation be educated about the vitality of security. We therefore propose a role-based security awareness model to be implemented for South African hospitals.

4.2 A Role Based Awareness Model

The proposed model is depicted in Figure 1.

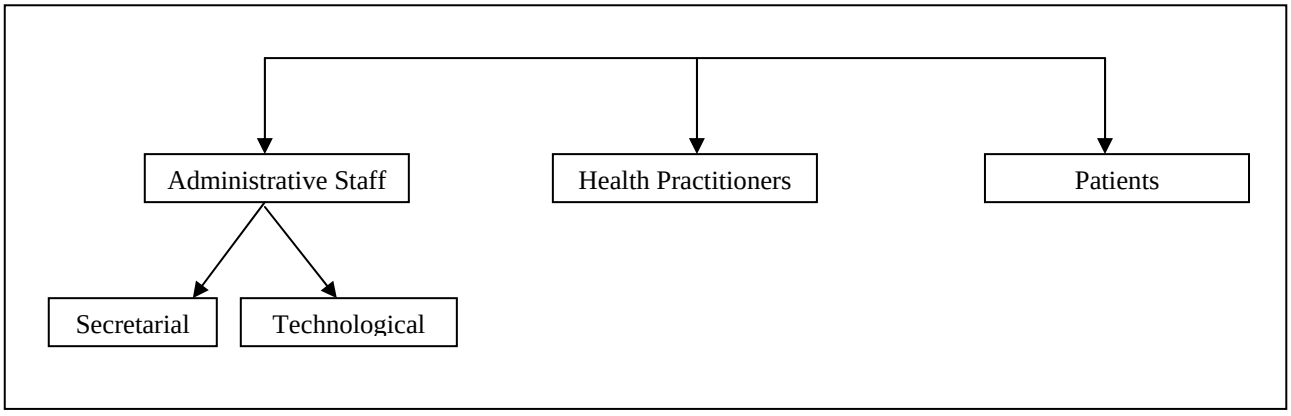

Figure1. A Role-Based Security Awareness Model

The model that is proposed will address role-based awareness as its title implies. In our study we are taking a look at a hospital, be it private or public. The hospital usually consists of health practitioners and administrative staff.

Health Practitioners: These are the people that look after the patients, day in and day out. They diagnose, talk about confidential issues with the patients and handle the sensitive records of the patients. It is imperative that they are aware of privacy issues that relate to the patients.

Administrative Staff: These are divided into two sections, the secretarial and the technological staff. The secretarial staff deal more with patients checking in and checking out. They can also check patient records for specific doctors, but only to a specific level. They are the weakest link. The Technological Staff are more concerned about computer security and information security. They do not deal directly with the patients, but more with patient data that is stored on the hospital's computer systems.

Awareness as an element from SETA that is intended to allow individuals to recognise IT security concerns and respond accordingly. As the learner is the recipient of information in awareness activities, it is increasingly important that the programme targets the audience that it is intended for. This will maximize the benefits achieved from such a programme. It is pointless running a programme for all staff, where most of the information is too generic or too specific to be applicable.

If an organisation's awareness program is properly designed, developed and implemented; it is only left to the employees to make certain that technology is being used properly. In order for technology to work, it needs people.

4.3 Sample Questionnaires

From the literature survey that we have carried out, we have deducted that there is a need to have a security awareness checklist in the health sector. This checklist will be distributed to several role-players at hospitals that fall under the private or the public sector. It will be limited to administrative staff and health practitioners. It will be addressing issues that pertain to the patients' privacy whilst they are within the boundaries of the hospital as well as what happens during the time that leads them to being there and when they have left. These issues will be viewed from the patient's perspective, the health practitioner's perspective as well as the administrative staff's perspective.

Accordingly, some questions are listed which could form a part of the awareness checklists.

4.3.1 Administrative Staff: Technological

1. Are all departmental staff aware of security processes?

2. Did the staff receive computer security awareness training?

3. Are staff members aware of the Privacy Policy and their responsibilities?

4.3.2 Administrative Staff: Secretarial

1. Do you regularly have education sessions that focus on aspects of privacy, confidentiality or security to promote best practice in your area?

2. Do staff members know where the privacy website is located on the Intranet?

3. Are medical records left unattended in your work area?

4.3.3 Health Practitioner: Doctor

1. Do you use fair and lawful ways to collect personal information?

2. Do you have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it?

3. If a patient asks, what sort of personal information you hold about them, what purposes you hold it for and how you collect, use and disclose that information. Do you take reasonable steps to let them know?

4.3.4 Health Practitioner: Hospital Manager

1. What measures will be taken to ensure the personal information is secure during transit and storage?

2. Will the personal information be used for any secondary purposes?

3. Have all the staff members in the medical practice been reminded of good personal health information management? It may be appropriate for all family practice staff to sign confidentiality agreements related to their use of personal health information.

4.3.5 Patient

1. When your personal health information was collected, did the Health Practitioner ensure that you are aware of the reasons as to why they are collecting your personal information?

2. Are you able to access your own personal health information in an appropriate way?

3. Are you allowed to correct this information using a process that tracks any amendments?

5 CONCLUSION

This paper took a look at the reformation of the South African health sector that has been initiated by the South African Government. We compared these developments with what is already available out there internationally. It was realised that the South African health sector needs a checklist to ensure that all the role-players are sufficiently aware of issues pertaining to the security and privacy of health information. Hence we proposed a role based security awareness model. This model ensures that all role players in the health sector are targeted according to their level and method of exposure to and utilization of health information. With the level of privacy awareness being very low in the South African health sector, designing a role-based SETA program by making use of the proposed role based awareness model would ensure that this problem is addressed aptly.

6 REFERENCES

ANC. (1994a). *A National Health Plan for South Africa*, African National Congress, Johannesburg, South Africa.

ANC. (1994b). *A National Health Plan for South Africa.* Retrieved June 1, 2006 from http://www.anc.org.za/ancdocs/pr/1994/pr0101d.html.

Asia, B., Pillay, Y. (2003). *Districts and Development: National Newsletter, July 2003*. Retrieved March 14, 2006, from ftp://ftp.hst.org.za/pubs/govdocs/dhs/dhs0703.pdf.

Buckovich, S.A., Rippen, H.E., & Rozen, M.J. (1999). *Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information*.

Bush, G. W., President: United States of America. (2004). *State of the Union Address, January, 20, 2004*. Retrieved April 23, 2006, from http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html.

Canadian Biotechnology Advisory Committee. (2004). *Biotechnology and the Health of the Canadians*. Retrieved March 16, 2006, from http://cbac-cccb.ca/epic/internet/incbac-cccb.nsf/vwapj/BHI-Final_Dec-13-04-E.pdf/$FILE/BHI-Final_Dec-13-04-E.pdf.

Committee on Standardization of Data and Billing Practices. (2003). *Recommendations of the Committee on Standardization of Data and Billing Practices.* Retrieved April 19, 2006, from http://www.medicalschemes.com/publications/ZipPublications/Presentations%20And%20Reports/StandardisationManual.pdf.

Department of Health. (2004). *Strategic Priorities for the National Health System, 2004-2009.* Retrieved November 22, 2005 from http://www.doh.gov.za/docs/policy/stratpriorities.pdf.

Department of Health. (2006). *Strategic Plan 2006/07 - 2008/09.* Retrieved March 14, 2006, from http://www.doh.gov.za/docs/misc/stratplan/2006-2009/foreword.pdf .

Department of Health. (n.d.). *Health Sector Strategic Framework 1999-2004: Socio-Economic and Health Status.* Retrieved June 9, 2006 from http://www.doh.gov.za/docs/policy/framewrk/chap02.html.

Federal Agency Security Practices. (2000). *Information Security and Privacy Training for [the Agency] Information System Security Officers*. Retrieved March 16, 2006 from http://www.iwar.org.uk/comsec/resources/fasp/ISSO-course-slides.ppt.

Health Technology Assessment. (n.d.). *Discussion Document on a Strategy for the Future*. Retrieved November 22, 2005, from http://www.sahealthinfo.org/hta/htadiscussion.pdf.

Hedberg Calle. (2003). *2003 South African Health Review. Health Information Systems Progress with Caveats – an Integration Perspective*. Retrieved September 2, 2005 from http://www.hst.org.za/uploads/files/Information_Systems.pdf.

Herold, Rebecca. (2003). *Information Security and Privacy Awareness Materials Design and Development*. Retrieved April 4, 2006, from URL:htttp://www.delcreo.com/delcreo/free/docs/Awareness%20Materials%20Design%20and%20 Development.pdf.

Institute of Health Systems. (n.d.). *Health Informatics*. Retrieved March 16, 2006, from http://www.ihsnet.org.in/HealthInformatics/healthinforma.htm.

Mbeki Thabo, President: South Africa. (2005). *Presidency Department Budget Vote*. May 2005.

McDonald, M.D. (n.d.). *Health Information Infrastructure in Developing Countries*. Retrieved March 16, 2006, from http://www.greenstar.org/GHI/Developing%20Countries.htm

MediaPro. (n.d.). *Privacy Direction 101: Awareness*. Retrieved April 4, 2006, from http://www.mediapro.com/products/corpComp/pdf/PD101%20Product%20Sheet.pdf.

National Department of Health. (2004). *The Closed Health Broadcast Channel*. Retrieved March 14, 2006, from http://www.doh.gov.za/docs/pamplets/chbc.pdf.

National Department of Health. (2005). *Strategic Planning Newsletter No 3, November 2005*. Retrieved April 20, 2006 from http://www.doh.gov.za/docs/newsletter/stratplan/nov05.pdf.

Shaw, V. (2002). "The Development of an Information Systems for District Hospitals", *Proceedings of the 7th IFIP 9.4 Working Conference*, Krishna, S. and Madon, S. (eds.), Bangalore, India.

South African Information Technology Industry Strategy Project. (2002). *ICT Diffusion and ICT Applications in Usage Sectors Executive Summary*. Retrieved March 14, 2006, from http://www.trigrammic.com/downloads/ICT%20Diffusion%20-%20Executive%20Summary.pdf.

The Privacy and Security Working Group. (2003). *Report and Findings June 5, 2003*. Retrieved March 16, 2006, from http://www.connectingforhealth.org/resources/pswg_report_6.5.03.pdf.

The White House. (2004). *Transforming Health Care: The President's Health Information Technology Plan*. Retrieved April 23, 2006, from http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html.

United States Department of Health and Human Services. (2004). *News Release: Secretary Thompson, Seeking Fastest Possible Results, Names First Health Information Technology*

Coordinator. Retrieved April 22, 2006, from http://www.hhs.gov/news/press/2004pres/20040506.html.