THE PROTECTION OF PUBLIC HEALTH DATA

- A CASE STUDY -

S. Nkundla[a], D. Pottas[b], M.M. Eloff[c]

[a] School of Information Technology, Border Technikon, South Africa
[b] Faculty of Computer Studies, Port Elizabeth Technikon, South Africa
[c] School of Computing, UNISA, South Africa

[a] snkundla@ingulube.bortech.ac.za, +27 43 702 9251, Private Bag X1421, East London, 5200
[b] dalenca@petech.ac.za, +27 41 504 9100, Private Bag X6011, Port Elizabeth, 6000
[c] eloffmm@unisa.ac.za, +27 12 429 6336, PO Box 392, Unisa, 0003

ABSTRACT

South Africa's health system consists of a large public sector and a smaller but fast-growing private sector. Health care varies from the most basic primary health care, offered free by the state, to highly specialized health services available in the private sector for those who can afford it. The responsibility for the overall performance of a country's health system lies with government, which in turn should involve all sectors of society. Government has the responsibility for establishing the best and most equitable health system possible with available resources. Various studies and surveys during recent years have highlighted that public hospitals in South Africa are in a precarious state. Corruption, staff shortages, deteriorating infrastructure, increased centralization, equipment failures and shortages, and an increased influx of (especially HIV/AIDS) patients, have all been identified as factors contributing to a progressively worsening public health-care situation.

With less resources and more poor people, cash-strapped provinces like the Eastern Cape face greater health challenges than wealthier provinces like Gauteng and the Western Cape. A case study was conducted at a public health organization in the Eastern Cape to examine the perception of resident health-care professionals and administrative staff on the status of the health systems and the privacy and confidentiality of patient data at the hospital. The availability, accessibility and usability of patient information were primary points of investigation. Several procedural and systemic inadequacies were identified which lead to the conclusion that there is a problem with the protection of public health information.

This paper provides feedback on the survey conducted at the hospital and analyses the value of patient data within the framework of the critical characteristics of information. The role of government and information technology in ameliorating the situation is investigated.

KEY WORDS

Public health systems, critical information characteristics, legal and ethical issues

THE PROTECTION OF PUBLIC HEALTH DATA

- A CASE STUDY -

1 AN OVERVIEW OF THE SOUTH AFRICAN HEALTH SYSTEM

"A health system is a combination of resources, organisation, financing and management that culminate in the delivery of health services to the population" (Roemer, 1991). South Africa's health system consists of a large public sector and a smaller but fast-growing private sector. Healthcare varies from the most basic primary healthcare, offered free by the state, to highly specialised health services available in the private sector for those who can afford it.

Statistics obtained from (safrica.info, 2003) paint an interesting picture. The public sector is under-resourced and over-used, while the mushrooming private sector, run largely along commercial lines, caters to middle- and high-income earners who tend to be members of medical schemes (18% of the population), and to foreigners looking for top-quality surgical procedures at relatively affordable prices. The private sector also attracts most of the country's health professionals. R3, 5bn is spent on healthcare in SA, with 20% of the population being looked after by private hospitals and the other 80% being treated at public hospitals. Public health consumes around 11% of the government's total budget, which is allocated and spent by the nine provinces. How these resources are allocated, and the standard of healthcare delivered, varies from province to province. With less resources and more poor people, cash-strapped provinces like the Eastern Cape face greater health challenges than wealthier provinces like Gauteng and the Western Cape.

The responsibility for the overall performance of a country's health system lies with government, which in turn should involve all sectors of society. Government has the responsibility for establishing the best and most equitable health system possible with available resources. Various studies and surveys during recent years have highlighted that public hospitals in South Africa are in a precarious state. Corruption, staff shortages, deteriorating infrastructure, increased centralisation, equipment failures and shortages, and an increased influx of (especially HIV/AIDS) patients, have all been identified as factors contributing to a progressively worsening public healthcare situation (EthicSA, 2000). In mitigation of these factors, a district-based health system is being developed to ensure local-level control of public health services, and to standardise and co-ordinate basic health services around the country to ensure that healthcare is affordable and accessible to everyone (safrica.info, 2003).

Government recognises that IT provides immense opportunities for improving delivery of services. It relies on the State Information Technology Agency (SITA) set up four years ago to deliver IT services to government. SITA is a government-owned company to which the state outsources a large part of its IT requirements and pays for those services. SITA is in the difficult position of having to deliver profits to government, but also to provide it with a good service.

Healthcare reform has placed an even greater importance on the use of information technology (IT) and hospital information systems (HISs) within the hospital environment to assist *in providing more efficient and effective care* (Harris, Kiefert, 1999). This statement is particularly relevant in the South African context. Therefore, it may be asked what the status quo is with regard to IT and HISs in South Africa. Do these systems contribute to service delivery and more importantly, are the nature of the systems and procedures such that public health data is protected? As a starting point to answering these questions, a case study was conducted at a public healthcare organisation in the Eastern Cape.

2 CASE STUDY

A case study was conducted at a public hospital in the Eastern Cape to examine the perception of resident healthcare professionals and administrative staff on the status of the health systems at the hospital and the protection of their patient information. The availability, accessibility and usability of patient information formed a primary focus of the investigation. The case study findings are based on information gathered through semi-structured interviews and questionnaires distributed to administrative staff and healthcare professionals (doctors and nurses) at the hospital.

2.1 Survey Results

The questions posed in the questionnaire, were mainly geared towards assessing the computer literacy of respondents, accessibility of patient information and perceptions about patient information privacy and confidentiality.

The survey respondents included 20 healthcare professionals and administrative staff. The results are depicted in Figure 1 and Figure 2. From the results, the following main points can be stated:

- 80% of the respondents had never used a computer before. This result would lead to an assumption that the healthcare professionals and administrative staff at the hospital are in need of computer skills training.
- A very high percentage (95%) of staff agreed that patient folders are not readily available.
- 70% of staff concurred that patient information is not easily accessible.
- All staff indicated that there is no IT department in the hospital. This was a surprising statistic since there certainly is an IT contingent at the hospital in the form of a SITA agency.
- A lack of communication between departments in the hospital was identified by 60% of the staff.
- Patient information privacy and confidentiality was primarily rated as poor (45%) and very poor (20%).

Further salient points raised during the interviews, include:

- lack of support with computer-related problems and of a more general nature,
- poor working conditions, shortage of staff, and lack of equipment.

2.2 Management of Patient Information

The following description is intended to provide insight into the processing of patient information at the hospital where the case study was conducted. When a patient reports to the hospital reception desk, the following procedure is followed (Chief Admin Clerk, 2003):

- The reception clerk determines whether the patient has been at the hospital before. If it is a new patient, a new folder is created and a folder number is allocated. If the patient already has a folder, the folder is fetched from the folder / filing room. However, sometimes folders are lost, in which case the clerk will create a new folder for that patient.
- The patient takes the folder to the nurse and is examined. If the patient does not need to be admitted to the hospital, a prescription is provided (where relevant) and the medication is issued at the dispensary. If the patient is to be admitted, a referral is made to a doctor.

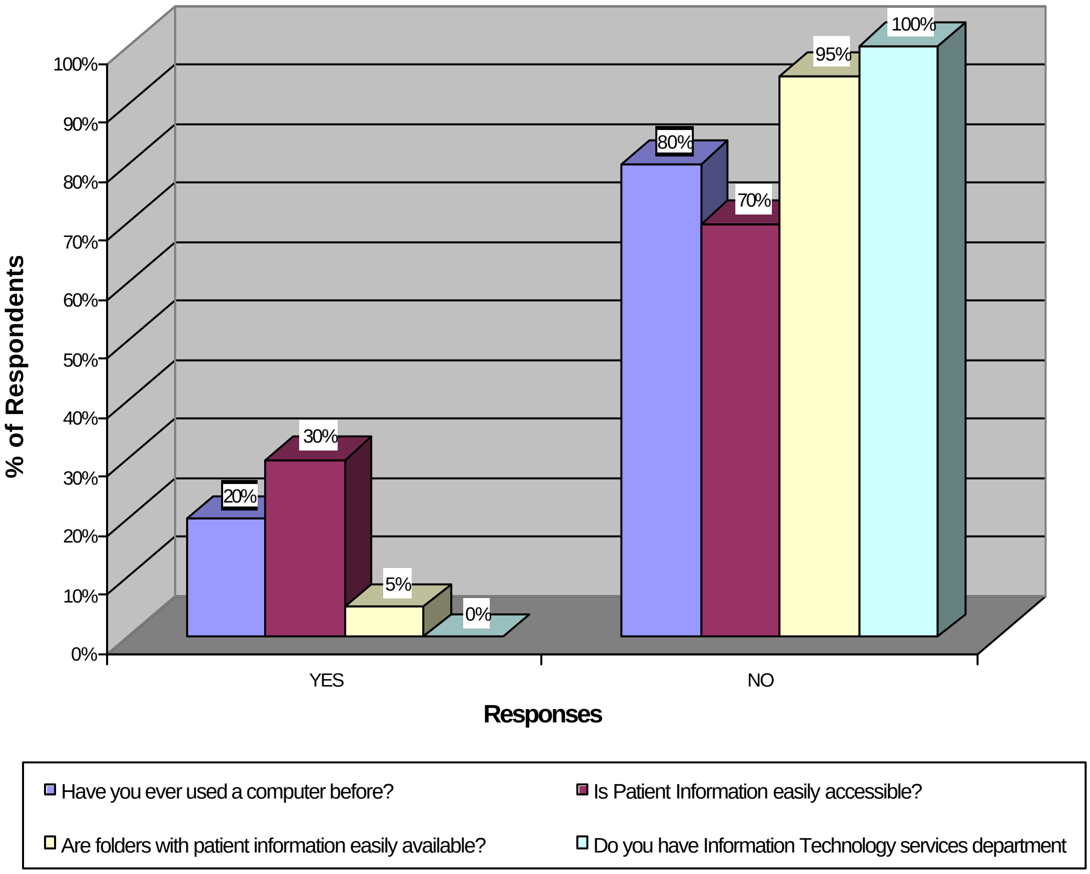

Figure 1: Questionnaire – Responses to YES / NO questions

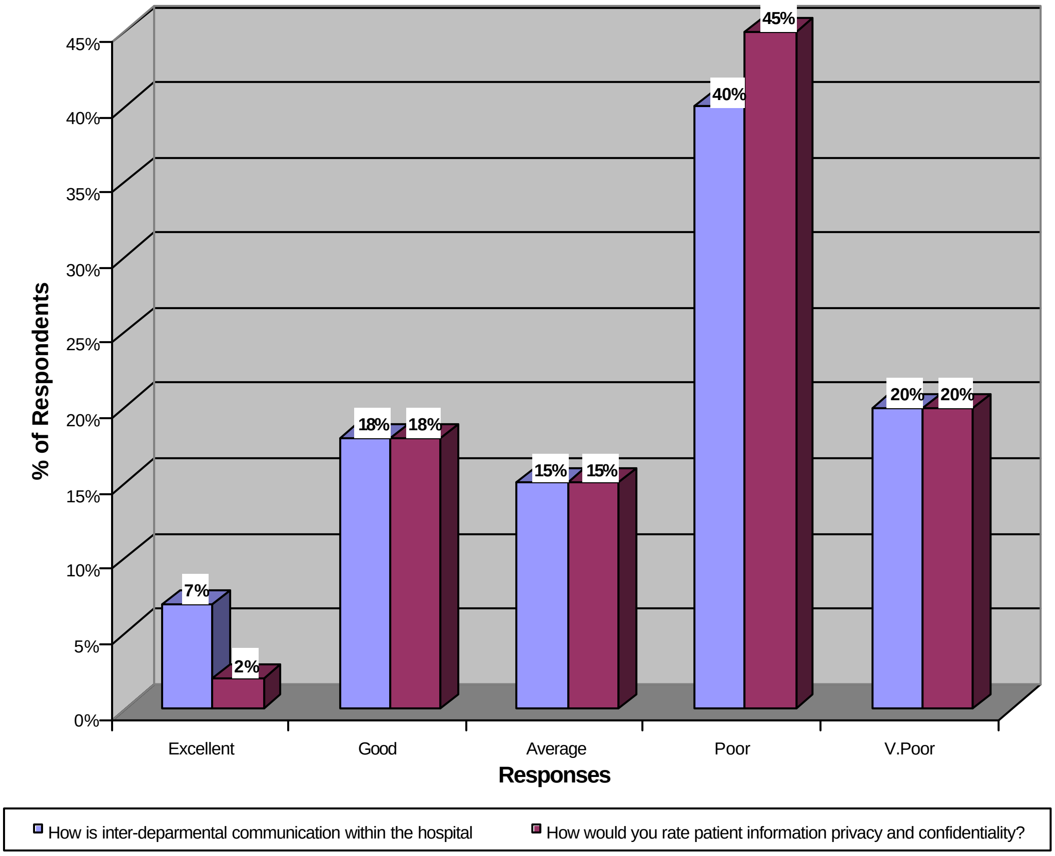

Figure 2: Questionnaire - Responses to RATING questions

- The doctor will create a pink folder for a patient to be admitted. He then phones the ward department to make a booking for a bed.
- In the wards, the nurses and doctors record all patient information in the patient's folder.
- If x-rays must be done, the nurse or doctor authorises it and the patient will go to the pathology department for the x-rays. In this department patient information is computerised.
- After the patient is discharged, (s)he goes to the finance department to pay or make payment arrangements. In the finance department, patient information is computerised to facilitate the management of account payments.
- From the finance department, the patient must return the folder back to the ward department. From here the folder will be returned to the folder / filing room.

From this procedure, some concerns may be raised:

- Data redundancy and information inconsistency

  A folder might be lost either by a patient or by a health-care professional. This leads to multiple folders being created for one patient. Furthermore, since folder numbers are not computerised, these numbers can be assigned to different patients.
- Partial computerisation of patient information

  From the discourse above, it is clear that the computerisation of patient information is not an end-to-end process. Healthcare information systems should be geared to supporting patient care from a holistic point of view. Ideally these systems should support cost-effective decision-making for administrative people as well as clinical decision-making for physicians (Tähkäpää et al, 1999).

In summary, patient data is improperly collected and not efficiently used in this government hospital. It is not uncommon for data (files) to be lost or incorrectly interpreted. Computerisation of patient data is applied in a fragmented fashion, which does not contribute to the holistic use and management of patient data. Harris (Harris, Kiefert, 1999) states that overall information technology diffusion in hospitals in the United States seems to be progressing, but it does not seem dominating. Financial or business management type applications seem to have preference over applications dealing with the quality and effectiveness of patient care. This corresponds to the use of the HIS at this hospital in the Eastern Cape, which is primarily used for the capturing of data for financial purposes.

The problems identified by the case study and the subsequent concerns that have been raised, can be further analysed from an information security perspective. How do these problems reflect on the critical characteristics (confidentiality, integrity, availability, etc) of patient information?

3 THE CRITICAL CHARACTERISTICS OF PUBLIC HEALTH INFORMATION

Information has value if it complies with and retains certain critical characteristics. Historically, the C.I.A. (confidentiality, integrity and availability) triangle, which identifies such characteristics, was strongly associated with information security. Whitman and Mattord (2003) propose a robust model of the characteristics of information that is more apt for today's computing environment with its constantly evolving threats. This model is applied to the public health information scenario in subsequent discussions with some examples from the case study.

3.1 Confidentiality and privacy

Confidentiality ensures that computer-related assets are accessed only by authorised parties (Pfleeger, Pfleeger, 2003). Only those that have been allocated the necessary access rights should be able to access the relevant information.

Government and country laws are responsible to keep medical records and patient information confidential. For many decades the vast majority of the South African population has experienced either a denial or violation of fundamental human rights, including rights to health care services. To ensure the realisation of the right of access to health care services as guaranteed in the Constitution of the Republic of South Africa (Act No. 108 of 1996), the Department of Health is committed to upholding, promoting and protecting this right and therefore proclaims the PATIENTS RIGHTS CHARTER as a common standard for achieving the realisation of this right. The Data Protection Act of 1998 provides protection for personal data. This includes information, which by itself or in conjunction with other easily obtainable information can identify a specific person.

Closely related to the characteristic of confidentiality, is the characteristic known as privacy. The prospect of storing health information in electronic form raises concerns about patient privacy based on two concepts (Mauro, 2003):

- The individuals' fundamental right to control the dissemination and the use the information about themselves.
- The information about an individual, revealed to someone not willingly designated by the data subject, may be used to harm his or her interests.

The privacy of an individual (from a medical data perspective) addresses the protection of that individual's personal health information (ie mental and physical condition) from access by unauthorized individuals. Patients expect a certain level of privacy in public hospitals. In our increasingly intrusive society, however, personal privacy is often seen as under threat. Such a threat has the potential to disrupt an individual's ability to maintain significant relationships that help to define that individual's personality. Physicians, nurses and hospital administrative staff have a duty to maintain in strictest confidence any personal information obtained in a professional capacity.

Confidentiality is a fundamental principle as it provides patients with health care choices free of outside influence; it empowers patients by giving them control over who will have information about their health condition and it enables them to seek help without fear of public knowledge. Unauthorised access to patient information is the single major threat to privacy in health care environments. Patient information must be available only on a ‘need-to-know’ basis. As IT is used more frequently as the basis for patient records, health care providers will need to increase their awareness of the need for information security.

3.2 Integrity

The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption to its authentic state (Whitman, Mattord, 2003). This characteristic is not only under threat from external forces. Authorised users who have access rights to the data must be restricted so that their input truly represents the real world events.

Assume that a patient’s allergy information is entered on a hospital information system. The integrity of such information is of extreme importance. If somebody wants to sabotage the hospital and they change this data, the patient could be exposed to allergens, which in a worst-case scenario, could lead to death. This would lead to medical malpractice suits and the reputation of the hospital would be irrevocably damaged. Thus the integrity (trustworthiness) of certain data in the medical scenario is of utmost importance.

3.3 Availability

The characteristic of availability refers to the fact that information will be available to users when they need it and how they need it. This was assessed as being particularly problematic in the case study, which is symptomatic of the partially paper-based system used at the hospital. In such an environment where crucial decisions are based on the information in patient folders, it is inconceivable that availability should be a problem. Patient information should always be available to authorised users. When patient information is not readily available when needed, a hospital could potentially face chaos. In the case study, loss of availability has been identified in the form of the loss of patient folders. This leads to an overburdening of the administrative staff who have to create new folders.

3.4 Accuracy

When information is accurate, it has no errors and it contains the content that the user expects. Consider the information contained in a patient folder as an example. If a physician bases a clinical diagnosis on information contained in such a folder, subsequent life or death is not an exaggerated outcome of such an action. Therefore, the accuracy of the information in the folder is of crucial importance.

In the case study, the existence of multiple patient folders for a single patient is an example of loss of accuracy. Depending on which folder is located at the time of treatment, that version of the information will be taken as truthful. If the first folder is located and used, then the patient record inaccurately reflects the clinical history of the patient (assuming that the second folder contained a record of further clinical diagnosis not included in the first folder).

3.5 Authenticity

Information is authentic when it is the information that was originally created, placed, stored, or transferred. It has to conform to fact or reality. If a patient has two files, then one cannot say that the information in either of the files is not authentic. Both files were created as true reflections of the patient's data at the time of creation. Should a *patient* enter information on a folder in a section reserved for input from a health professional, then that information is not authentic. The information was misrepresented – it does not conform to reality because a physician or a nurse did not enter the information.

3.6 Utility

If information is available to a user, but the format is not as expected, it is not useful as it cannot serve the indented purpose. For example, in the case study, the settling of accounts is procedurally handled as a computerised business process. If a patient's data was not computerised, it is available but is of no use as pertaining to utility in the context of the management of account payments. The most severe case of loss of utility could lead to a loss of availability. For example, if a patient's HIV status is stored in encrypted form and the key is lost, all the critical characteristics of the information are still upheld. The information is still (very) confidential and available (the key was lost not the information). Certainly it is still accurate and authentic and possession has not been breached. However, it cannot be used, so utility is lost. If the key cannot be recovered, then the scenario could be described as a loss of availability.

3.7 Possession

An example of loss of possession would be if a patient decides to take his or her folder home in stead of returning it to the next point of delivery, as required. The folder contents will not necessarily be disclosed (loss of confidentiality), but there is a loss of possession. In this case there will also be a loss of availability if the patient returns to the hospital without the folder.

In this section, the critical characteristics of information were analysed as pertaining to the protection of public health information. This provides a comprehensive framework within which information security should be addressed in order to ensure that information has value and is secure.

The collection, storage and use of health information must be done with an understanding of confidence and trust and used (only) for the purpose of effective and efficient patient care. This leads to the question of ethics and legal issues in the medical profession.

4 LEGAL AND ETHICAL ISSUES

Patient information is accessed and used by many people in different departments within a hospital. Some use it for work purposes, while others violate patient rights by using the information illegally. The spread and use of Information Technology has created many ethical issues. Public health information raises some difficult legal and regulatory issues as well. Therefore it is important to include a discussion of legal and ethical issues pertaining patient information in this discussion.

Turban, McLean and Wetherbe (1999) explain ethics as a branch of philosophy that deals with what is considered to be right and wrong. It involves morals and making choices or judgments about what should or should not be done. An ethical person behaves and acts the right way. Ethical issues need to be taken into account when implementing health information systems.

The duty of confidentiality is one of the most commonly articulated ethical obligations to patients, but it is also the one most subject to breach on behalf of the state. Ethical values vary by society, and from person to person within a society. What is ethical to one person might be unethical to the next person. People confuse ethics with religion. Religion is based on personal notions about the creation of the world and the existence of controlling forces or being (Turban et al., 1999).

Many companies and organisations in South Africa develop their own codes of ethics. Turban et al. (as quoted by Oz, 1994) defines a code of ethics as a collection of principles intended as a guide for members of a company or an association. An attempt to organise these issues into a framework was undertaken by Mason (1986) and Mason et al. (1995), who categorised ethical issues into four kinds: privacy, accuracy, property, and accessibility (Turban et al. 1999). In South Africa, doctors are required to pledge adherence to The World Medical Association's (WMA) Declaration of Geneva, which states that doctors must take the health of their patients to be their first consideration and that they must treat them without discrimination. All healthcare professionals (nurses, doctors and admin staff) should adhere to this code of ethics.

The risk of misuse of patient information rises proportionately with the ease of access to information. Worldwide, there is a gap in legislation covering this area and it is becoming more and more urgent that legislation is introduced to control it.

Legal issues facing the development of electronic health records are complex. The law outlines what health care professionals may engage in, in the use of patient information. Negligence is an unintentional wrong. The person fails to act in a reasonable and careful manner and thereby causes harm to the person or property of another. As a healthcare professional, legal responsibility (liability) for actions is a given. What you do or do not do can lead to a lawsuit if harm results to the person or property of another. Information about a patient's treatment cannot be given to others except when the provision of this information is approved in writing by the patient or as otherwise allowed by law. Some examples of circumstances in which patient information can be provided to others according to the law include the sharing of information between professionals who are treating the same patient, to provide information to insurance companies and other third party favors (eg police), by order of the court.

5 GOVERNMENT AND THE ROLE OF IT

Information Technology (IT) covers everything from designing software and managing information systems to training and supporting those who use them. Information technology has become the major facilitator of business activities in the world today. It is rapidly changing the way individuals live, firms do business, governments administer and nations interact. Information technology is not only changing the way hospitals operate, but it is also changing the relationship between medical professionals and patients. Certainly it is known that delivering an efficient and effective service depends to a great extent on the management of health information.

It is reasonable to expect that computers be available for health-care professionals (doctors, nurses and admin staff). Every department in a hospital must have computers and these computers must be integrated from one department to another. The integration of computers from one department to another within a hospital improves the accessibility, availability and usability of patient information. Secondly it is intended to contribute to the improvement of internal communication between employees within a hospital. The successful implementation and use of hospital information systems will ensure accurate, secured patient information and time will be used effectively when it comes to processing information relating to patients.

Technology can also assist hospitals and other medical institutions faced with critical staff shortages to reduce errors - be they medication, prescription transcription, order, administration or dosing errors. Technology will help simplify the care process, limit the duplication of work and patient information, improve communication, improve patient care documentation compliance and provide additional decision support tools (Powe, 2003). IT plays a very important role both in private and public organisations or sectors. However it has both positive and negative effects in organisations. Computerisation of patient information can be a waste of time and money unless there are clear reasons for use and adequate technical and user support. Without a system that is primarily patient-centric, there can be no effective service delivery, and hospitals will struggle to enjoy time and cost savings.

Harrison (Harrison, Boulle, Ramduny, 2003) states, "… as there is a roll-out of computer installations in health services in South Africa, the following points should be noted:"

- Computers have the potential to improve work efficiency and communication.
- We need to shift away from the use of computers primarily by administrative personnel to their use by health service managers and health workers.
- District and facility managers should be computer literate and have access to word processing, computing and electronic communication.
- Computer infrastructure and installation must be appropriate. For example, expensive networks and satellite link-ups are not a priority in facilities without water, fridges, good drug supplies or equipment.
- Technology frequently obscures the main focus, which is communication.

The demand for cost-effective healthcare solutions is growing in South Africa, as delivery costs spiral upward and patient expectations of specialist care rises (International Trade Center, 1998).

Therefore the role of government as a healthcare funder is very important. The philosophy of the government is to develop a unified health system capable of delivering quality healthcare to all the provinces efficiently and in a caring environment. Government is trying by all means to support the demands of public hospitals in South Africa, however it is not easy as South Africa is still a developing country.

In the recently released World Health Organisation Report for the year 2000, South Africa ranks 57th when it comes to the availability of funding and resources for health, yet in terms of the efficiency of healthcare delivery, South Africa takes 175th place (CADRE, 2003). Government alone cannot address the development and growth challenges in our public hospitals. Healthcare professionals, admin staff and patients must collectively take responsibility for the success of this partnership.

Geraldine Fraser-Moleketi (Fraser-Moleketi, 2003) states that the increasing role of information technology in government offers an integral tool for the strengthening of state institutions. This recognition represents a certain step in the right direction.

6 CONCLUSION

This paper presented the results of a case study conducted at a hospital in the Eastern Cape, the results of which posed some serious flaws pertaining to the security and privacy of patient data. An analysis of the critical characteristics of information was conducted to highlight the value or lack of value of information if these characteristics are not maintained. The role of information technology and the government were investigated as facilitators in the proper use and management of public health information.

The value in this research lies not in purporting a solution to a specific problem, but rather as an enabler for awareness of the lack of IT diffusion and the subsequent problems experienced in a South African public healthcare institution. A next step would be towards conducting research on a national level to determine the status of IT diffusion nationally and the subsequent impact on the protection of public health information.

7 REFERENCES

CADRE, *The response of government: Policy and interventions, fiscal and financial issues* [online]: Available on the Internet: http://www.jointcenter.org/international/hiv-aids/1_government.htm (Referenced 23/August/2003).

Chief Admin Clerk. Interview. 2/May/2003. 2 hours. Hospital in the Eastern Cape.

EthicSA. [online]. *Chris Hani Baragwanath Hospital Ethics Audit*. Available on the Internet at: http://www.ethicsa.org/article.php?story=20030919084251975 (Referenced 1/April/2004).

Fraser-Moleketi, G. 2003. *Selected Media Articles: Government opts for open source* [online]. Available on the Internet at:
http://www.sita.co.za/news/selected_media_articles/opt_open_source.htm
(Referenced 4/July/2003).

Harris, A.L., Kiefert, P. (1999). Information Technology Diffusion in Hospitals in the United States. In *Proceedings of the Information Resources Management Association International Conference*. Hershey, PA, USA, 1999.

Harrison, D., Boulle, A., Ramduny, V. *A District Communication Strategy for Health* [online]. Available on the Internet at: http://www.hst.org.za/isds/kwikskz/kwik3.htm. (Referenced 15/August/2003).

International Trade Center: Health Services. 1998 [online]. Available on the Internet at : http://www.intracen.org/servicexport/sehp_health_services.htm (Referenced 22/August/2003).

Mauro, V. *Patients privacy and economic interests: raising issues in health telematics*. LUISS Guido Carli University [online]. Available on the Internet at: http://cersi.luiss.it/Articoli/veleth.PDF. (Referenced 12/May/2003).

Patients Rights Charter. Available on the Internet at : http://www.hst.org.za/doh/rights_chart.htm (Referenced 30/June/2003).

Pfleeger, C.P., Pfleeger, S.L. (2003). *Security in Computing*. Third Edition. Prentice Hall PTR. 2003.

Powe, L. CSC Press Releases: *Technology could ease stress of nursing shortage*. 07/April/2003 [online]. Available on the Internet at: http://za.country.csc.com/en/ne/pr/680.shtml (Referenced 13/September/2003).

Roemer, M.I. *National health systems of the world. Vol. I The countries; Vol. II Issues*. New York and London, Oxford University Press, 1991; 1993.

safrica.info. *Health care in South Africa [Online]*. Available on the Internet at: http://www.safrica.info/ess_info/sa_glance/health/health.htm (Referenced 11/July/2003).

Tähkäpää, J., Turunen, P., Kangas, K. (1999). Information Management in Public Healthcare: A Case of a Small Municipality Federation. In *Proceedings of the Information Resources Management Association International Conference*. Hershey, PA, USA, 1999.

Turban, E., McLean, E., Werthebe, J. 1999. *Information Technology for Management: Making Connections for strategic Advantage*. 2nd Edition. New York: John Wiley and Sons. Inc.

Whitman, M.E., Mattord, H.J. (2003). *Principles of Information Security*. Thomson Course Technology. 2003.