Community Awareness and Involvement: An Overlooked Security Control

N. Ruxwana[1], M. Herselman[2] and D. Pottas[1]

[1]School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.
[2]Meraka Institute, CSIR & Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: mherselman@csir.co.za

Abstract

The implementation of Information and Communication Technologies (ICTs) in the healthcare industry has witnessed a tremendous growth in the recent past. These ICTs are often viewed as vehicles that can bridge the digital divide between rural and urban healthcare centres. They hold the promise of bringing resolution to the shortages facing the rural healthcare sector by introducing e-health solutions such as electronic health records, telemedicine and e-education. Furthermore, e-health solutions promise to improve efficiencies, reduce costs, and improve the quality of health service delivery. Therefore, ICTs have proved to be increasingly fundamental to the socio-economic development of nations. However, these e-health solutions are currently under-realised in developing countries, especially in rural areas due to various challenges. Developing countries face barriers to reach significant levels of e-health adoption. Existing research, in identifying these barriers, has grouped a variety of contributing factors into several categories. This study, in viewing these categories, highlights an overlooked factor which impacts e-health development and other ICT4D activities in the rural areas of South Africa. Community awareness and involvement, at an appropriate level, is presented as an important control that may reduce or even eliminate the prevalence of e-health solutions vandalism and theft in rural areas. The literature case reviews and main author experiences are mainly based in the rural areas of the Eastern Cape Province in South Africa.

Keywords

Community, Awareness, Involvement, e-Health Solutions, Vandalism, Theft, Security

1. Introduction

The implementation of Information and Communication Technologies (ICTs) in the healthcare industry by the various stakeholders of e-health, has witnessed growth in the recent past. These ICTs are often viewed as vehicles that can bridge the digital divide between rural and urban healthcare centres, and they hold the promise of bringing resolution to the shortages that face the rural healthcare sector by introducing solutions such as e-health, telemedicine and e-education (Ruxwana et al., 2010). Key among the implementation opportunities is the use of the Internet to enhance healthcare communication and service delivery. Chelley (2001) asserts that "the advent of the information infrastructure or information technology revolution and its unprecedented capabilities to process, store, refine and disseminate data,

information and knowledge in a variety of ways across borders, has dramatically changed the ways in which governments, the public and private sectors operate World-Wide".

Over the past decade, the need to develop and organize new ways of providing efficient healthcare services has been accompanied by major technological advances. This has resulted in a dramatic increase in the use of ICT applications in healthcare, collectively known as e-health. According to Eysenbach (2001), e-health is an emerging field at the intersection of medical informatics, public health and business, with referral and information delivery enhanced through using the Internet and related technologies. The author states that in a broader sense, the term characterises a technical development and a state-of-mind, a way of thinking, an attitude, and a commitment to networked, global philosophy to improve healthcare locally, regionally and globally by using ICTs.

The key drivers for e-health implementation are, according to Chu (2007), quality, safety, effectiveness, and efficiency of healthcare services. As a result, there has been an increase in e-health solutions developments in South Africa, and other developing countries. Electronic medical records, hospital information systems, public networks, health decision-support, expert systems, telemedicine, community health information systems, the use of the Internet and other technical systems have altered the cost, quality, accessibility and delivery of healthcare (ADF, 2001; Braa and Hedberg, 2002; Seebregts and Singh, 2007).

E-health developments are viewed as a vehicle that can bridge the digital divide between rural and urban healthcare centres. They promise to facilitate the resolution of shortages that face the rural healthcare sector (Ruxwana et al., 2010). They have the potential to significantly and irrevocably change healthcare services delivery and patient care and introduce applications that facilitate the management of healthcare systems throughout the world (Louw & Hanmer, 2002). In addition, e-health improves efficiencies, reduces cost, and improves the quality of health service delivery (Wen & Tan, 2003).

Thus, ICTs are widely perceived to have the capability, if used effectively, to help bridge a variety of social and economic gaps that divide rural and urban communities, including access to healthcare services (Gurstein, 2005). ICTs can be used to assist rural communities and healthcare centres to obtain a degree of service more comparable to the range of services offered by healthcare centres in urban areas. They have the potential to enhance the wellbeing of underprivileged people in many ways including empowerment, education and skills sharing and to deliver expanded healthcare services to rural communities such as those in the Eastern Cape Province of South Africa, which is the area of focus of this study.

In most of the developed world, the community enjoys the benefits brought by e-health solutions and are involved with innovative ways to capitalize on e-health potentials. However, the e-health solutions opportunity is under-realised in developing countries, especially in rural areas due to several challenges. One of the many challenges of e-health in rural areas is the issue of security. This paper

recognizes a lack of community awareness and involvement as one of the factors that pose a threat to the security of e-health solutions. Therefore, the paper promotes community awareness and involvement, at an appropriate level, as a remedy to selected security challenges of e-health solutions in rural areas. The literature case reviews and main author experiences are mainly based in the rural areas of the Eastern Cape Province in South Africa.

2. Rural Challenges and e-Health Promises

It is widely accepted that a large percentage of the global population lives in rural areas. This is evident in developing countries, especially in Africa. In concurrence, ITU-D Group 7 (2000) maintains that more than half the global population in 2000 lived in rural areas. According to Kawasumi (2000), rural areas can be characterised by any one of the following:

- Lower levels of economic activity with limited job opportunities; the existing economic structure may be based mainly on agriculture, fishing or handicrafts if they exist.
- Challenging topographical conditions, such as lakes, rivers, hills, mountains, deserts and long distances between settlement areas, which cause the construction of wired telecommunication networks to be costly.
- Severe climatic conditions that make heavy demands on certain components of telecommunications equipment, for example, antennas and remote switches add to the costs of installation and maintenance in rural areas.
- Lack or absence of public facilities, such as usable water, reliable electricity supply, access roads, regular transport, and an existing communication infrastructure.
- Underdeveloped social infrastructure, such as health, education or small business.
- Low per-capita income, due to limited jobs and economic activities.
- A scarcity of relevant skills which challenges the technical maintenance and support of any implemented ICT solution.

These characteristics lead to several challenges that relate to the implementation of ICTs in rural areas. It becomes more difficult to provide public telecommunications services of an acceptable quality, by traditional means, at affordable prices, while achieving commercial viability for the service provider. This becomes more burdensome for areas that possess most or all of the rural characteristics, such as the rural areas in the Eastern Cape Province of South Africa.

The Eastern Cape is one of the poorest provinces in South Africa and is composed of many underdeveloped rural areas. Thom (2007) states that this province is known as, “home to the poorest districts in the country”. Palmer et al. (2002) confirms that low per-capita income, low levels of economic activity, scarce technical personnel, an underdeveloped social infrastructure, and difficult topographic conditions are characteristic of the Eastern Cape. In addition, Ruxwana (2009) confirms that the lack of infrastructure and technical personnel in the rural areas has implications for

the maintenance and repair of technical equipment placed in such communities, such as the equipment for telemedicine solutions in rural hospitals.

The Eastern Cape Department of Health (ECDOH, 2006), in an attempt to overcome the challenges facing their healthcare sector, is committed to attracting appropriately qualified, potential employees to areas with the greatest needs in service delivery. The ECDOH further aims to retain employees through a program of compensation and personal development to sustain quality healthcare, and to implement e-health solutions through telemedicine programs that support education, training and academic services. However, the Eastern Cape health system continues to be plagued by challenges such as staff shortages, poor management and weak primary care, coupled with high levels of poverty and unsatisfactory access to basic services such as piped water (Thom, 2007). The province has embarked on projects to implement various e-health solutions, while attempting to overcome many of its disparities, and is focusing mainly on telemedicine solutions in the rural areas.

According to Field (2002), telemedicine describes the use of electronic information and communications technology to provide and support healthcare when distance separates the participants. The notion of telemedicine emerged as the practice of using audio, visual and data communications for medical consultations, diagnosis, treatment, nursing care, medical education and transfer of medical data (Mathur, 2003). Medical services provision using telemedicine include both treatment and diagnosis (Wooton et al., 2006). The categories of telemedicine include real-time and pre-recorded telemedicine. Pre-recorded telemedicine involves a store and forward mechanism. Information is gathered, stored and later transmitted to the recipient and the results are transmitted back to the sender. Real-time telemedicine allows participants to send and receive information almost instantly.

The Internet plays a significant role in both real-time and pre-recorded telemedicine. For instance, video conference transmissions in real-time telemedicine are made possible through the Internet. Store and forward applications use the Internet to transmit images (e.g. the digital transmission of x-ray images). Thus, e-health enhances the communication between patients and doctors, and facilitates education through online resources and information sharing irrespective of their locations (Eysenbach, 2001). However, this requires using ICTs as the backbone to support communications. There is a need for complex infrastructure and the deployment of sophisticated equipment, such as computers, servers, digital cameras, software and similar. These requirements pose their own set of challenges relating to e-health security.

3. e-Health Security Challenges

Although, there are many ICTs that are developed to facilitate communication processes, enhance health service delivery and to overcome the challenges faced by rural areas, ICTs have their own challenges. In addition to the challenges previously stated, ICTs are faced with security challenges. There exist many security threats to ICTs such as information breaches by intruders, malicious programs like viruses and worms and physical threats. These threats can cause severe damage.

The Eastern Cape Department of Health, as previously stated, has embarked on projects to implement e-health solutions in rural areas in an attempt to overcome its healthcare challenges. E-health solutions communicate and exchange medical information between doctors or patients using video conferencing, emails, or web-based messaging services (Pagliari, 2005). These communications involve sensitive information transmitted either through wired or wireless media. Thus, security is a priority to ensure that communications are protected from security breaches. The communicated information is highly confidential and may jeopardize the privacy of the patient if it is compromised.

The healthcare sector, according to Katsikas et al. (2008), is quickly exploiting ICTs for the provision of e-health services. However, according to their recent surveys, one of the severest barriers to the adoption rate of e-health is the lack of security measures that are required to assure both service providers and patients that their relationship and transactions are carried out privately, correctly, and timely.

Sharma et al. (2006) also acknowledges the significant developments in the healthcare sector. There has been a paradigm shift, at a national level, of the attention, resources and interest towards e-health. However, the authors maintain that e-health, though exciting and promising, presents new challenges, particularly with regards to acceptable standards, choice of technologies, overcoming traditional jurisdictional boundaries, up-front investment and privacy and confidentiality.

Although e-health provides attractive solutions to the challenges faced by the health care sector, especially the shortage of healthcare practitioners where the telemedicine solution has proved to have potential, the way in which it should be practised has not been resolved (Jack & Mars, 2008). According to Jack and Mars (2008) the WHO resolution of 2005 acknowledges the need to respect the principle of equality and differences in culture, education, language, physical and mental ability and geographic location (World Health Assembly eHealth Resolution [WHA 58/28]: 2005, cited by Jack & Mars, 2008), but it does not address specific ethical issues, such as the lack of direct patient-practitioner contact, informed consent, confidentiality, safety, data security and the legal implications of the cross-border, international practice of e-health solutions, such as telemedicine (Edworthy, 2001; Jack & Mars, 2008). Thus, Jack and Mars (2008) maintain that there are no functional ethical guidelines for the practice of telemedicine in South Africa, as there seem to be gaps found in the South African DOH's Telemedicine System regulatory, named "Telemedicine Code of Ethics and Professional Conduct", which appears to have been adapted from a code of conduct for commercial telemedicine product providers and not healthcare professionals (Jack & Mars, 2008).

Of these ethical issues highlighted to have not been covered, the need for security appears even more critical as the physician, according to Mars and Scott (2010), must always ensure that patient confidentiality and data integrity are not compromised. Thus there is a need to ensure that the e-health data must be secured to prevent access by unauthorized persons (Mars & Scott, 2010).

Security is, according to Li and Hoang (2009), a critical requirement for the e-health system because the system allows the sensitive information of the patient to be accessed remotely, which may make the entire e-health system vulnerable to malicious attacks. Therefore, security becomes an integral part to enhance the delivery of health services as promised by these e-health solutions.

In the literature, there are several studies that focus on the issues of information security and ICTs security in general. Most of them focus on security models within the application and communication, technological and organizational aspects of security, where the security services required to secure the communications were identification, authentication, access control, integrity, confidentiality, and availability (Smith, 2005; Blobel & Roger-France, 2001; Tulu & Chatterjee, 2003; Marković (2006); Doupi, et al. 2005; Gupta & Gupta, 2001; Bobadilla et al., 2007; Sulaiman et al., 2008).

This paper focuses on physical security aspects, where the e-health solutions implemented in rural areas are in jeopardy of being vandalised or stolen. This affects the e-health solution's quality and sustainability and leads to an excessive loss of resources, which are already limited in rural areas. Although there are several motives for these malicious acts, this paper maintains that community awareness and intervention, at an appropriate level, is one of the critical factors that should not be overlooked when implementing e-health solutions in rural areas.

4. Community Awareness and Involvement: Remedy to e-Health Security Threats

Although e-health solutions provide the potential for rural areas to improve healthcare service delivery, their deployment is challenged by several aspects mostly relating to lacking ICT infrastructure. However, the implementation of these ICT infrastructures in rural areas is complex and expensive. In the Eastern Cape Province, this is compounded by vandalism and theft (Chetty et al., 2006; Tucker, 2008; Tucker & Blake, 2007; Mandioma, 2007).

There is evidence in literature that there are physical security threats in regard of ICTs that are implemented in rural areas. These studies highlight that a major issue relating to wired technologies in remote/rural areas in South Africa is the high prevalence of copper cable theft, plus there is the probability of poor-quality copper cables being installed (Lowe et al., 2000; Daily Dispatch, 2005; Daily Dispatch, 2005; DeMartino, 1999).

One of the major barriers, according to Mandioma (2007), to telephone service provisioning in the Eastern Cape Province rural areas, is the malicious theft of copper telephone cables. He further maintains that physical security is important and should be taken into consideration during the deployment of the network in such rural areas to help safeguard the network and to minimize vandalism of the equipment on the deployed network.

In concurrence, a recent study conducted on technology use (specifically services delivered via Vodacom mobile phones) by Small and Medium Enterprises (SMEs) in rural areas in the Eastern Cape Province, found that of all the challenges posed in the operation of these services, those relating to theft of mobile phones surpassed those relating to the use of the technology itself (Mazibuko et al, 2008).

Another case is the attempt by Telkom to implement Digitally Enhanced Cordless Telephones (DECT) in the Qumbu village, between Tsilitwa and Sulenkama, which has not been successful for a number of reasons. Rated above the unreliable power supply, were vandalism and theft (Tucker, 2008; Chetty et al, 2006). Furthermore, physical security was evidenced to be the prevalent challenge in the implementation of the Digital Doorway in the Eastern Cape Province. Major challenges were reported from experiences during the inaugural Digital Doorway installation in South Africa which was completed in 2002 in Cwili, a rural village outside the mouth of the Kei River in the Eastern Cape. These include the lack of technical expertise in the communities, extreme environments, illiterate or non-English speaking users, vandalism and maintenance costs. But the most serious problem the team faced was the theft of the video server (Cambridge et al, 2008).

To combat the challenges of ICT infrastructure for e-health solutions, various alternatives have been proposed and piloted. Wireless infrastructure proved to be less susceptible to theft or vandalism, as may be the case with copper lines. Wireless also has the added benefit of being usable for portable and mobile applications, as well as fixed ones (Chetty et al., 2006. Tucker, 2008; Tucker & Blake, 2007). Digital cameras were introduced for solutions such as telemedicine, and they proved to be more flexible. An additional benefit of such cameras is their small size and robust construction, allowing use in a variety of clinical situations. This also simplifies transport to remote areas and protection from damage or theft (Fraser et al, 2001). Although these measures eliminate vandalism, to some extent, they on the other hand bring a greater responsibility to alert those who are using them of security cautions and ways in which these can be taken care of to prevent theft. This can be achieved by instilling the value and the impact these have to their community, especially the benefits they bring for healthcare services.

The latest advancements, according to Martin et al. (2002), in Internet security technologies such as data encryption, electronic signatories and firewalls, leads to healthcare users being more willing to adopt the Internet due to its potential benefits, such as increased efficiencies, lower cost, easier access to media-rich information and knowledge and faster decision making.

However, Katsikas et al. (2008), assert that a large number of individuals are not willing to engage in e-health or only participate at a reduced level because they do not trust the e-health solution and the underlying ICTs to be secure enough. This paper is of the opinion that there are numerous benefits to be realized and trust to be gained from e-health solutions' users when the solutions are properly implemented. It is important that the hosting healthcare community is aware of the objectives of the e-health solutions and its benefits to their lives. The lack of awareness about such e-health solutions has lead to resistance against their use, which imposes security

threats to the e-health solution because it can lead to vandalism or theft of such solutions.

In contrast, Mandioma (2007) is of the opinion that community awareness leads to theft. In his study on Internet aspects in rural areas in the Eastern Cape, it is apparent that when alternative sources of energy, such as solar energy and generators, are implemented to mitigate the power supply challenges in rural areas, there is prevalent theft of such technologies. He further reveals that community awareness of the use and application of solar power has led to an actively fraudulent market for solar panels. As a result of the stolen equipment, some sections of the networks were permanently affected, thus depriving the rural communities from accessing the Internet (Mandioma, 2007).

An important lesson in terms of community awareness and involvement is to be learnt from the experiences of the Digital Doorway initiative (Cambridge et al., 2008). Instead of selecting communities and then expecting them to take ownership, communities have to apply for a Digital Doorway, since this leads to greater long term ownership and commitment.

Mandioma (2007) maintains that the results of his research indicate that community engagement must be done in the right way and at the right levels. In concurrence, this study maintains, as according to Rycroft et al. (1997) that the most successful anti-theft mechanism has been the education and involvement of local communities (Rycroft et al., 1997; cited by Mandioma, 2007). However, it must be noted that in any communication or knowledge sharing, there is an acceptable level of knowledge sharing or involvement. For example, within the healthcare sector, there is sensitive information that must be kept confidential, and there is information that can be shared with the public. Similarly, when developing e-health solutions for rural health care, there needs to be a strategic decision, based on prior assessments, about whom in the community and at what level, should be made aware of what information.

There is evidence that community awareness and involvement, when implemented appropriately, enables ICT implementation sustainability, its security and its effective use. This has been the case in the rural MPCC, which is one of the successful ICT4D projects in the Eastern Cape Province, Dwesa. This solution has proved the benefits of ICTs and represents a turning point for the communities residing in these disadvantaged rural areas.

Community awareness need not contain any information that may be of threat or expose e-health solutions to vandalism, but the functionality and the benefits of the e-health solution to the lives, community, or their working environment should be made known. The level of involvement may be the use of champions or local leaders and local authorities.

5. The Lack of Community Awareness in e-Health Solutions

E-health solutions use equipment such a computers, digital cameras, servers, TV screens, etc. These are highly risky in rural areas where people have low income and

poverty persists. The equipment can easily be sold, and would bring some income to those who sell them, thus can be seen as an opportunity to make money. However, when people are aware of the role the equipment plays in their lives or in the community, it reduces the intent to harm.

During a study conducted on quality assurance methodologies for e-health solutions implemented at rural hospitals in the Eastern Cape Province, a number of relevant observations were made at five rural hospitals. It was observed that some hospitals had further security measures over and above the security guard at the main gate, such as surveillance cameras, burglar doors and windows, or ruggedized security protection, etc. However most of the hospitals (N=3) did not have additional security measures. In most cases the Mindset e-health solution was protected using various measures, while the other e-health solutions were not as protected.

It was also observed that computers are at times left unattended and unlocked, thus jeopardizing patient information as people can easily gain access to information through unattended, unlocked computers. Digital cameras were the most prevalent equipment used and were kept in unlocked drawers. This poses opportunities for them to be stolen as they can fit in a jacket pocket easily and one may leave the hospital premises without being searched for stolen goods. To some extent the cameras were not used as the link was not operational. This led them to be used for personal purposes, again exposing them to the threat of theft. Laptops are also made available to some professionals. Their (lack of) awareness of security and ways to protect the equipment as well as the data stored in them, were noted as problems.

The following threats are prominent when there is a lack of community awareness and involvement in rural areas:

- **Vandalism by community members**: this occurs when communities find technological equipment whose use they are unaware of. They find no importance of it and may intentionally vandalise it; with the notion that better services could be delivered rather than the money apparently wasted. Thus the activity has the intention to trigger the government or local authorities to take action.
- **Theft of equipment**: this occurs when the community is unaware of the value added by the e-health solution to their lives or communities. They find an alternate purpose for it and steal it for commercial purposes or just to have it stolen. Community awareness does not prevent this act, but assist in avoiding it through the involvement of community members guarding against such malicious acts.
- **Ignorance of the solution**: This is a twofold problem. It refers to ignorance by healthcare professionals about the value of e-health solutions. They disclose information or expose the e-health solution to the physical threat of vandalism or theft. Secondly, the problem exists at the community level. Communities may ignore malicious acts towards or theft of e-health solution equipment. When called upon to intervene, community leaders or local authorities, including the police, may not respond. This is because they are uninformed and unaware of the value of such equipment. They may

likely believe it is one of the wastages by the government, as is often referred to in rural areas when the value of solutions is unknown.

The afore-mentioned threats highlight physical security problems that may occur due to a lack of community awareness of e-health solutions in rural areas. These threats, though mild, could pose serious implications to e-health implementation, especially in rural communities where activities of this nature are common. Therefore, it is important for community awareness and involvement, at the right level, to be considered as part of the processes and methods used to implement e-health solutions in rural areas.

Awareness and Involvement Guidelines for e-Health Projects in Rural Areas

6. Awareness and Involvement Guidelines for e-Health Projects in Rural Areas

Recommendations for e-health implementation projects in rural areas are listed subsequently. At a minimum, the following guidelines should be followed:

- A security assessment to identify key security issues that can jeopardize or cause harm to the use of the solution.
- Training and awareness programmes to ensure that staff members are aware of the potential security risks and possible solutions.
- Awareness and involvement of the community both internal (within the healthcare facilities, focusing on healthcare workers) and external (local community members and authorities) to instil ownership and care of the solutions. At an internal level, this can be achieved by including local hospital management. For external communities, an appropriate level of leadership such as the use of champions or community leaders, can propagate awareness and thus gain acceptance, thereby improving security and ownership of e-health solutions. If local authorities are aware of the importance and value of e-health solutions, incidents of theft and/or vandalism may be afforded the necessary attention.
- Ensuring a means of enforcing compliance to security measures for the protection of equipment.
- Training on physical care and protection of equipment.
- Installation of physical security measures such as burglar doors and windows on the facilities with equipment, e.g. TVs, computers, etc. as well as for safe keeping of smaller devices such as laptops, cameras, PDAs, etc.

In addition to these project-specific recommendations, the following are recommended:

- The introduction of e-health solutions training as part of the curriculum for healthcare workers by education and training institutions to ensure that the significance and value of such solutions is understood. This should include modules that will make healthcare workers aware of potential security

threats of using e-health solutions and possible measures to mitigate these threats.

- A government directive addressing security measures and guidelines for e-health solutions, which should include suggested penalties for non compliance.

With particular reference to the community awareness and involvement aspect of these recommendations, it becomes clear that its scope covers not only the public, but also healthcare workers, community leaders and the local authorities who preside in a particular community.

Figure 1 depicts the entire probable stakeholder list for e-health solutions. As shown, the stakeholder list includes provincial government (in this case the Eastern Cape Department of Health). At this level, there must be influence exerted in terms of the importance of the security of e-health solutions, to ensure that district management and local hospital management effect security guidelines and measures. This, together with appropriate community awareness and involvement in e-health solutions, will contribute to decrease the prominence of theft and vandalism as major challenges of successful e-health solution implementation in rural areas.

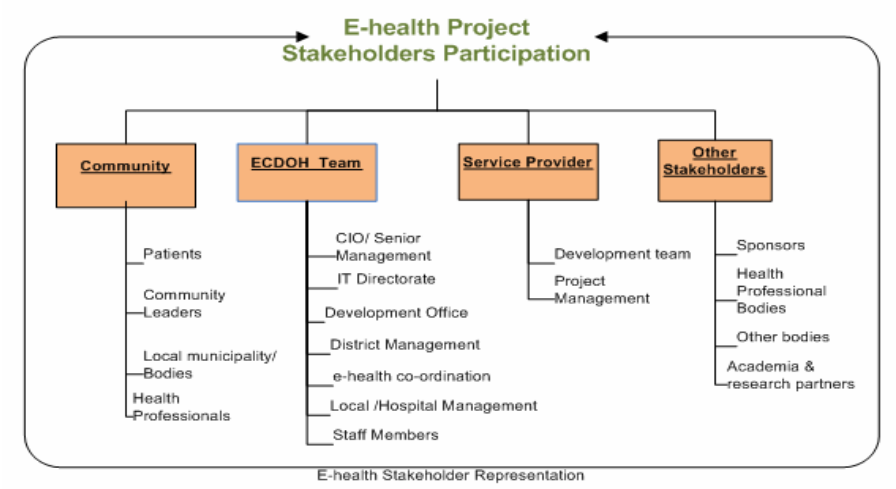

Figure 1: e-Health solution stakeholders

7. Conclusion

Information and communication activities are a fundamental element of any rural development activity (Islam and Hasan, 2009). However, developing countries face barriers in reaching significant levels of e-health adoption. This paper contributes to the knowledge pool, with the aim of making e-health implementations viable in rural communities. This is achieved by presenting the often overlooked challenge of e-health community awareness and involvement, and its implications to e-health solutions and physical security threats. The study presents community awareness and

involvement, at an appropriate level, as an important control that may reduce or even eliminate the prevalence of e-health solutions vandalism and theft in rural areas. This will bring new opportunities for rural people through facilitating successful adoption, rather than unapprised rejection of e-health solutions.

8. References

ADF. 2001. Information and communication technology for health sector. Available at: http://www.uneca.org/adf99/adf99health.htm#1 (Accessed: 24/06/2006).

Blobel, B., and Roger-France, F. 2001. A systematic approach for analysis and design of secure health information systems. International Journal of Medical Informatics, 62(1).

Bobadilla, J., Gomez, P., and Godino, J. I. 2007. Mapaci: A real time e-health application to assist throat complaint patients. Paper presented at the Internet and Web Applications and Services, 2007. ICIW '07.

Braa, J. and hedberg, C. 2002. The Struggle for District Based Health Information Systems in South Africa. The Information Society, p. 113-127.

British Educational Communications and Technology Agency (BECTA). 2003. "What the research say about ICT and Motivation". Available at: www.becta.org

Chelley, J. 2001. Information Technologies Quoted in PATH. Available at: www.rho-org/html/ict.

Chetty, M., Blake, E. and McPhie, E. 2006. VoIP deregulation in South Africa: Implications for underserviced areas. Telecommunications Policy. Volume 30, Issues 5-6, Pages 332-344.

Chu, S. 2007. Introduction to HL7 V3. 6th Asia-Pacific HL7 Conference.

Daily Dispatch. 2002. Copper Theft Costs Telkom R249m. Available at: http://www.dispatch.co.za/2002/10/23/southafrica/GCOPPER.HTM (accessed: 2010/01/15).

DeMartino, K. 1999. ISDN and the Internet. Computer Networks. Vol 31, pp 2325-39.

Dlodlo, N. 2009. Access to ICT Education for Girls and Women in Rural South Africa: A Case Study. Council for Scientific and Industrial Research. Meraka Institute: Advanced Institute for Information and Communication Technologies. Available at: http://researchspace.csir.co.za/dspace/bitstream/10204/3546/1/Dlodlo_d2_2009.pdf (accessed 2010/01/20).

Doupi, P., Ruotsalainen, P., and Pohjonen, H. 2005. Implementing interoperable secure health information systems. Stud Health Technol Inform, 115, 187-214.

Eastern Cape Department of Health (ECDOH). 2006. Health Indibano. Available at: http://www.ecdoh.gov.za/uploads/files/100806094905.pdf (accessed 13 August 2007).

Edworthy, S. 2001. Telemedicine in Developing Countries. Br Med Jl 2001;8:557–60.

Eysenbach, G. 2001. What is eHealth?. Available from: http://www.jmir.org/2001/2/e20/ (accessed: 2006/10/06).

Field, M. 2002. Telemedicine: A guide to assessing telecommunication in health care. National Academy Press.

Gupta, V., and Gupta, S. 2001. Kssl: Experiments in wireless internet security: TR-2001-103, Sun Microsystems Laboratories, of Sun Microsystems, Inc.

Gurstein, M. 2005. Why community technology matters: Community informatics and the effective use of ICTs. Community Informatics Research Network CIRN conference. Paper presented at the International Conference of the Community Informatics Research Network: CIRN2005 on Cape Town, 24-26 August 2005.

Islam, S.,and Hasan, N. 2009. Multipurpose community telecentres in Bangladesh: problems and prospects. The Electronic Library, 27(3), pp. 537-553.

ITU-D Group 7. 2000. New technologies for rural applications final report of ITUD Focus Group 7, 2000. Available at: www.itu.int/ITU-D/fg7/pdf/FG_7-e.pdf (accessed: 2010/01/15).

Jack, C.E and Mars, M. 2008. Telemedicine – A Need for Ethical and Legal Guidelines in South Africa. South African Family Practice, Vol 50, No 2.

Katsikas, S., Lopez, J. and Pernul, G. 2008. The challenge for security and privacy services in distributed health settings. Stud Health Technol Inform. 2008;134:113-25. PMID: 18376039 (PubMed - indexed for MEDLINE).

Kawasumi, K. 2000. New Technologies and Solutions for Rural Accessibility. Last Rapporteur for ITU-D-Focus Group 7. Available at: http://webworld.unesco.org/infoethics2000/documents/paper_kawasumi.Rtf (accessed: 2009/11/12).

Li, W. and Hoang, D. 2009. "A new security scheme for e-health system". 2009 International Symposium on Collaborative Technologies and Systems. CTS pp.361-366, available at: http://doi.ieeecomputersociety.org/10.1109/CTS.2009.5067502 (accessed: 2010/01/15).

Louw, J.A. and Hanmer, L. 2002. Implications of the Information Revolution for Economic Development in South Africa Project Code: A.1.009. DTI. Available from: http://www.trigrammic.com/downloads/Health%20Information%20Flows.pdf (Accessed: 01/11/2006).

Lowe, R. and Arevalo-Lowe, C. 2000. Accessing the Internet –DSL, Cable Modem or Dial up. Available at: http://www.webhero.org/System/access.asp (accessed: 2009/11/12).

Martin, S., Yen, D.C., and Tan, J.K. 2002. E-health: impacts of internet technologies on various healthcare and services sectors. International Journal of Healthcare Technology and Management, Volume 4, Numbers 1-2 / 2002. pp. 71 – 86.

Marković, M. 2006. On secure e-health systems. Paper presented at the CENEX-SDC Project International Conference, PSD 2006, Rome, Italy.

Mathur, A. 2003. The role of information technology in designs of healthcare trade. Available at: http://www.icrier.org/pdf/wp111.pdf, (accessed 9 September 2008).

Mitchell, J. 1999. From telehealth to E-health: The unstoppable rise of E-health John Mitchell & Associates for the Federal Australian Department of Communications. Information Technology and the Arts (DOCITA).

Mandioma, M. 2007. Rural Internet Connectivity: A Deployment in Dwesa-Cwebe, Eastern Cape, South Africa. Msc-Dissertation. Department of Computer Science Centre of Excellence in Developmental E-Commerce University of Fort Hare Alice, South Africa.

Omekwu, C. 2003. Current Issues in Accessing Document Published in Developing Countries, MCB University Press, Lagos. Available at: http://www.emeraldinsight.com/10.1108/02641610310477206 (accessed 2010/01/20).

Pagliari, C., Donnan, P., Morrison, J., Ricketts, I., Gregor, P., and Sullivan, F. 2005. Adoption and perception of electronic clinical communications in Scotland. Informatics in Primary Care, 13(2), 97-104(8).

Palmer, R.C.G., Timmermans, H. and Fay, D., eds. 2002. From conflict to negotiation: nature-based development on the South African Wild Coast. Special edition. HSRC, Pretoria, South Africa. ISBN 0-7969-1992-5.

Ruxwana, N.L. 2009. Technology assessment of rural hospitals in the Eastern Cape Province: knowledge, adoption, access, and availability of e-health solutions for improved health care services delivery in rural hospitals. Saarbrucken, Germany: vdm verlag dr. müller.

Ruxwana, N.L., Herselman, M.E. and Conradie, D.P. (2010). ICT applications as e-health solutions in rural healthcare in the Eastern Cape Province of South Africa. Health information management journal, Vol 39 no 1 2010. ISSN 1833-3583 (print) ISSN 1833-3575 (online).

Seebregts, C.J and Singh, Y. 2007. OpenMRS Workshop. In: HELINA COM. Available from: http://www.sim.hcuge.ch/helina/W1.pdf (Accessed: 22/01/2008).

Sharma, S.K., Xu, H., Wickramasinghe, N., and Ahmed, N.2006. Electronic healthcare: issues and challenges. International Journal of Electronic Healthcare. Volume 2, Number 1 / 2006. pg 50 – 65.

Sulaiman, R., Sharma, D., and Ma, W. 2008. A Security Architecture for e-Health Services. ISBN 978-89-5519-136-3, Feb. 17-20, 2008 ICACT.

Smith, R. 2005. Introduction to multilevel security. (Chapter 205) handbook of information security (Vol. 3): John Wiley.

Smith, E., and Eloff, J. H. P. 1999. Security in health-care information systems current trends. International Journal of Medical Informatics, 54, 39-54.

Thom, A. 2007. Eastern Cape limps along. Available at: http://www.healthe.org.za/news/article.php?uid=20031594 (accessed 13 August 2007).

Tucker, W.D. 2008. Internet Protocol-Based Tele-Consultation: A Voip Project. Citeseer. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.2059&rep=rep1&type=pdf (Accessed: 25/03/2010).

Tulu, B., and Chatterjee, S. 2003. A new security framework for hipaa-compliant health information systems. Paper presented at the Proceedings of Ninth Americas Conference on Information Systems, Tampa, FL.

Wen, H.J. and Tan, J. 2003. "The Evolving Face of TeleMedicine & E-Health: Opening Doors and Closing Gaps in E-Health Services Opportunities & Challenges". Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03).

Wooton, R., Patil, N.G., Scott, R.E. and Ho. K. 2009. Telehealth in the Developing World. Intern Develop Research centre.