International Conference on Information Society (i-Society 2014), Heathrow Marriott Hotel, London, United Kingdom, 10-12 November 2014

Information security risk measures for Cloud-based Personal Health Records

Avuya Mxoli[2], Mariana Gerber[1] and Nicky Mostert-Phipps[1]

1School of Information and Communication Technology Nelson Mandela Metropolitan University Port Elizabeth, South Africa

2Smart Systems Council for Scientific and Industrial Research Pretoria, South Africa

Abstract

Personal Health Records (PHRs) provide a convenient way for individuals to better manage their health. With the advancement in technology, they can be stored via Cloud Computing. These are pay-per-use applications offered as a service over the Internet. Similar to other Internet-based technologies, Cloud Computing poses security risks. This paper aims to formulate the implications of Cloud Computing risks on personal health information. A qualitative content analysis was used to analyse literature on Cloud Computing risks to emphasise its implications from a personal health information perspective. Access management, security issues, legal issues and loss of data are some of the risks that negatively impact the storing of PHRs in the Cloud. These can be mitigated by ensuring that only authorized parties are granted access; ensuring that users do not gain access to other users' data and that data remains encrypted; Cloud providers should comply to audits in order to make sure that proper regulations are followed in securing data in the Cloud; and making backups in case of data loss. Using Cloud-based PHRs can improve healthcare. Cloud Providers should work together with PHR providers in order to make sure PHR users can reap these benefits without being too concerned about the associated risks.