eJHI electronic Journal of Health Informatics
www.eJHI.net
2014; Vol 8(2):e10

Editorial – The changing face of ehealth security

Patricia A H Williams[1] **and Lizzie Coles-Kemp**[2]

[1] *eHealth Research Group, School of Computer and Security Science, Edith Cowan University, Joondalup, WA, Australia*
[2] *Information Security Group, Royal Holloway University of London, UK School of Computer and Security Science, Edith Cowan University, Joondalup, WA, Australia*

We are grateful to the Electronic Journal of Health Informatics (eJHI) for the opportunity to present this special issue on information security and electronic healthcare systems. Electronic health record (EHR) systems are notoriously difficult to design, and designing secure EHR systems is an even harder task. Part of the difficulty lies in the fact that the actual electronic health record is not simply the conversion of paper records into a digitised form. The EHR is often a re-engineering of healthcare services as the design takes advantage of the ability to “push the boundaries" of healthcare [1] and to transform the approach to the cycle of patient care. The healthcare professions have a long history of prioritizing the confidentiality of patient data. These professions also have long understood the relationship between maintaining patient privacy and maintaining patient trust. The provision of healthcare takes place in fluid, complex environments where the ability to deliver patient care is dependent on the quality and availability of patient data as well as on the facilities and skills of the healthcare provider. For these reasons, information security and the delivery of healthcare is intimately linked and has proven to be a fascinating challenge when designing electronic healthcare systems.

This special issue characterizes some of the contemporary challenges facing electronic healthcare system design. The topics presented in this special issue include the system design process, the governance framework, the access control model and the challenges related to the provision of cloud-based EHR services. This breadth reflects how information security affects all aspects of EHR design and deployment.

Williams and Coles-Kemp call for user-centered participatory design processes that help to bridge some of the design-reality gaps described by Richard Heeks and analyzable through Heeks’ ITPOSMO framework. The paper provides an example a communities of practice approach-based to identify and implement information security requirements as part of EHR systems. This example illustrates the positive results of using a culturally-sympathetic rather than a technology-focused design approach in EHR design.

Johnstone illustrates that whilst there are benefits to cloud-based service provision in the healthcare environment, there are also security issues that require attention. The paper provides an analysis of security issues in a particular case study, illustrating how information security is highly situated and methods are needed to understand security in context when new technical paradigms are put forward. Johnstone’s analysis demonstrates the need for specific cloud-service provision research in healthcare.

Williams and Mahncke present research that explores governance framework design and considers the implications of resourcing and security knowledge constraints on the design and provision of information security governance frameworks. The results of this research demonstrate the importance of language and simplicity of process for the success information security governance.

Gajanayake, Lane, Iannella and Sahama focus on the topic of access control: a subject that sits at the heart of all EHR systems. They propose a model that emphasises after the fact evidence and the important role that monitoring plays. The authors argue that this feature is necessary in order to encourage the development of appropriate ethics of use in EHRs.

This special edition of the eJHI provides an important contribution to the discussion on security in ehealth. The papers draw together important aspects of security that need to be embedded into EHR systems and the processes of governance that surround these. It is in-

creasingly important to being these issues to the fore and promote debate on the multi-facetted and complex area that is ehealth security.

References

1. Rigby M, Budgen D, Turner M, Kotsiopoulos I, Brereton P, Keane J, Bennett K, Russell M, Layzell P, Zhu F. A data-gathering broker as a future-orientated approach to supporting epr users. International Journal of Medical Informatics. 2007; 76(2): 137-44.

Correspondence

Associate Professor Trish Williams
trish.williams@ecu.edu.au

Dr. Lizzie Coles-Kemp
Lizzie.Coles-Kemp@rhul.ac.uk