electronic Journal of Health Informatics
http://www.ejhi.net
2008; Vol 3(1): e0

Special Issue: Health Information Privacy and Security

Anyone who works in the Healthcare sector understands the importance of maintaining confidentiality with a patient's personal and often highly sensitive information. This can be traced back to the 'Hippocratic Oath' (4th century BC) which defines the basis of ethics in medicine for our physicians. Translated from the original Greek, the penultimate paragraph defines the doctor's duty of confidentiality:
"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."

Since 'Hippocrates of Kos' founded the Hippocratic school of medicine our advancement of medical knowledge across the millenniums continues to escalate. Yet, this has not transpired through doctors and medics ensuring information was kept to themselves but by sharing their discoveries and knowledge. The confidentiality they practice encapsulates the values in the Oath by not spreading 'abroad', i.e. discussion about an individual's condition is confined within a practice or department for the primary purpose of helping the patient concerned. Any secondary use of this information that could advance our medical knowledge, for example, would not identify the individual concerned unless they consented to this.

The more recent advancement of shared knowledge through digital technology has provided a catalyst that is fuelling a revolution in both medical know-how and healthcare provision. But with this advance the traditional boundaries are being broken. The concept of confining information in written form to a physical location, such as a practice or surgery, is gradually disappearing. The remote and high speed access that today's digital technology brings presents new challenges and not only for healthcare providers but for governments, the ICT industries, lawyers and individuals. Patients are now being asked to give consent for access to information they may not have even been aware of. Or, worse still, through statutory requirements, they are now increasingly being informed when violations have occurred with their personal data held on computer systems.

The individuals as patients have a right to privacy over any personal and sensitive health data. They traditionally would talk to a doctor in confidence and assume that the associated healthcare organisation would be able to protect adequately their privacy. The knowledge required to keep a contemporary computer system secure is extensive and often beyond that of the healthcare practitioner. With the traditional boundaries being breached and the majority of personal computers in use not being specifically designed with security in mind, we certainly have our work cut out. Health informaticians are acutely aware of this, or at least should be, and need to engage in greater dialogue on the issues. In my opinion, those in denial are either hoping to avoid an acute problem or are seeking to gain financially by convincing others not to worry. Others may say this is just an implementation issue – what makes Health any different? – why not simply regard this as an IT security problem and leave it to the experts?

'Security' is focussed on keeping inappropriate and unauthorised people out (either physically or electronically). Whereas 'Privacy' is ensuring that only those that 'need to know' can access information and therefore has to operate both within and outside any firewalls that have been established to secure data. For example, consider remote access of your health records on a home computer; a firewall does not ensure privacy from other members of the family who have access to that machine. This concept applies to all computer systems across general practice, community care, hospitals and research institutions. Barriers are often in place to prevent unauthorised viewing within an organisation but often just at an application level. To consider whether this is sufficient then one needs to appreciate that any privacy violation can have lifelong consequences. That is, you cannot unlearn the knowledge that someone you may know personally has a mental or sexual health history. The fact is that the integrity of contemporary computer systems is more suited to the financial industries where the consequences of revealed data can be insured against and subsequently compensated for. More research and development work is needed before we can trust that our IT systems are sufficiently tuned to the specific requirements of healthcare and the many different people associated with that care.

The papers presented here in this special issue on 'Health Information Privacy and Security' highlight some

The *electronic Journal of Health Informatics* is an international journal committed to scholarly excellence and dedicated to the advancement of Health Informatics and information technology in healthcare. ISSN: 1446-4381

of the many special needs in healthcare. We now take for granted that sending emails is now an efficient and a relatively robust form of communication. With a web-based email application, security measures are going to be more demanding. Caffery *et al* provides an insight on how a system can be developed from OpenSSL to support a highly sensitive web-based email application with Paediatric and Adolescent mental health. A more general architectural approach for secure document circulation is addressed in the paper by Bracher *et al.* They focus on medical record privacy and how the organisation's privacy policies can be applied through trust relationships with the patients concerned. Liu *et al* consider the legal requirements for health information systems by reviewing some of the key advances across the international spectrum. In particular, this paper highlights the requirements of the Common Criteria in assessing IT products and systems with a view on its application for health to include recommendations on how to future-proof our systems for ongoing security measures. De la Motte and Harnett's paper considers the tricky issue of patient consent. Often legislation gives the patients certain privacy rights over their data but the patient is not normally the end-user of the systems deployed. Their paper shows how a client-task based approach can achieve privacy while providing the necessary levels of integration and access control without the need for IT staff intervention. O'Keefe's paper looks at the secondary use of health data for research purposes. The technical review of five different systems, employed in two countries, focuses on privacy preservation with the assumption that appropriate governance structure and security is in place. The review acknowledges that each system has its place depending on the research work being carried out and provides an evaluation for different scenarios. For secondary use of health data we must protect the identity of the individual. The use of computer data sets can increase the opportunity to use statistical means to identify individuals through inference. That is, by selectively focussing on known characteristics and identifiers such as postcode, age, etc. then the subject of the data can often be inferred. Anonymity can be preserved by not returning results where the number of records identified in a search fall below a predetermined value, i.e. 'k'. Li *et al* show some techniques for using k-anonymous data release and considers the limitation for this increasingly popular technique. Hence, comparison with 'secure multiparty computation' is given as an alternative privacy preserving data mining technique so that the compromise between security and efficiency can be judged. The concern over IT privacy and security in the clinical workplace has been addressed by Fernando and Dawson. They focus on the important issue of effective workplace training. Through questionaries they have established that current approaches were inadequate and were undermining the confidence that clinicians would have in any unified national programs for e-health information systems. The final paper by Josang asks us to consider trust with the online world of healthcare provision. The word and mouth opinion about the local doctor and their practice is losing its applicability in today's mobile and online society. This paper looks at how an online reputation system can be applied for the health sector to empower the consumer on decisions of trust with health care providers.

These papers highlight the fact that we are faced with a topic that can be complex, wide ranging and often emotive. Over time I expect to see different disciplines emerge from within Health Privacy and Security to address the differing requirements between data usage. Already this is happening to some degree between secondary research usage and primary care but the understanding across the community to distil effectively these topics is still limited. That is, continued evidence of over protection of health data sources by primary users is preventing secondary access. Hence, for the foreseeable future these topics will need wide ranging discussion across the scientific community and the general public. Hopefully some of the misconceptions have been adequately addressed here regarding what we can achieve with IT security and how that alone cannot provide the various types and levels of privacy needed for a trusted health information system.

Correspondence

Professor Peter Croll
Information Security Institute, QUT, Brisbane
Chair of Health Informatics Society of Australia (HISA) Privacy and Security SIG (HIPS)
Email: croll@qut.edu.au

Biography

Professor Peter R Croll
PhD, FACS, FBCS CITP, CEng.

Peter Croll is a research leader in Health Informatics with over 30 years' experience in ICT serving both industry and academia. At QUT he holds the chair for Software Engineering in the Faculty of IT where he directs the e-health research group focusing on risk and trust management of health information systems. He works closely with CSIRO's E-Health Research Centre on collaborative projects. This includes a recent National Fellowship to support their Flagship on Preventative Health to investigate the privacy and security risks associated with electronic health data integration. His previous roles have included the directorships of an ICT research institute and an IT research centre, Head of School of IT and Computer Science and an academy director. He is currently a Fellow of both the Australian and the British Computer Societies, a Chartered IT Professional and a Chartered Engineer. Peter Croll has over 100 refereed publications in books, international journals and conferences to include a citation in the IMIA 2007 year book. He is currently a member of the technical committee for the Australian Law Reform Commission's review of the Federal Privacy Act, a Board Director of the Health Informatics Society of Australia (HISA) Ltd. and he chairs the QLD branch of HISA and the national forums for HIPS and ehPASS that focus on Health Informatics Privacy and Security. Recently, Peter has established Better Life ICT a consultancy company to provide ICT expertise for eHealth products and services.