

QUT Digital Repository:
<http://eprints.qut.edu.au/>



Croll, Peter R. and Croll, Jasmine (2007) Investigating risk exposure in e-health systems. *International Journal of Medical Informatics* 76(5-6):pp. 460-465.

© Copyright 2007 Elsevier



ELSEVIER

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

Investigating risk exposure in e-health systems

Peter R Croll^{a,*}, Jasmine Croll^b

^a Information Security Institute, Queensland University of Technology (QUT), 126 Margaret Street, Brisbane, Qld 4001, Australia

^b Faculty of Health, Queensland University of Technology (QUT), 126 Margaret Street, Brisbane, Qld 4001, Australia

ARTICLE INFO

Keywords:

Personal health records
Acceptability of health care
Public health informatics
e-Health
Risk analysis

ABSTRACT

Purpose: Health managers, administrators and health practitioners now face new challenges due to the increasing dependency being placed on electronic health information systems. This paper focuses on Electronic Health Records for determining the critical attributes for e-health system development. The proposed QUiPS model aims to provide a framework for building trustworthy solutions by identifying the pertinent issues needed to determine the risk exposure with a given system.

Approach: To produce dependable, low risk and viable IT solutions, each critical attribute needs to be specifically addressed and prioritized. It is shown how these attributes possess a number of interdependencies making the analysis and prioritization tasks complex and hence, in practice, often incomplete. Two Australian case studies are presented that access enterprise level applications of live health records where these risk based techniques have been applied.

Results: The value and the shortcomings of taking a risk based approach to developing and deploying electronic health information systems that are safe and secure, is evaluated. The case studies presented indicate that traditional methods used to derive the requirements are often inadequate and the risks that are faced in ensuring a safe and secure system are highly application dependent and dynamic.

Conclusions: Convergence towards a viable universal solution for our electronic health records is not imminent and trust in e-health is fragile. Policies that data custodians follow need to be flexible and updated on a regular basis. Technological solutions are at best a stop gap to avoid the common hazards associated with access control and secure messaging. A wider range of analysis techniques to determine the key issues for a dependable health information system can derive longer term sustainable solutions.

© 2006 Published by Elsevier Ireland Ltd.

1. Introduction

Health care within Australia is a complex mix of private, public, state and federal provision. The need for continued investment in e-health is evident with the necessity to move from what has been a highly manual, diverse and widely distributed collection of health data to standardized, highly available and connected electronic record systems. To date, most data has been collected and stored as manual records

but the increased use of electronic records introduces new risks, particularly from the remoteness and speed of access that is now achievable. Appropriate use of technology can, for example, reduce the risks of incidences associated with common security weakness. Approaches to IT security is well understood, e.g. the Common Criteria [1]; plus its application to secure e-health is well researched [2–4]; which now has to take into account the recent legislative constraints, e.g. HIPAA [5]. Whatever methods are used, e.g. CORAS, CRAMM [6], the

* Corresponding author.

E-mail address: p.croll@qut.edu.au (P.R. Croll).

1386-5056/\$ – see front matter © 2006 Published by Elsevier Ireland Ltd.

doi:10.1016/j.ijmedinf.2006.09.013

software products must operate in a particular environment with particular external impacts resulting in a unique set of interconnected hazards and problems.

With the increased push toward national health data integration in Australia, e.g. Health Connect [7] and the problems of differing state and organizational policies any risks are far from static. For example, the National e-Health Transition Authority notes that privacy protection in Australia is a complex patchwork. “NEHTA’s position has been to chart health privacy requirements within the privacy environment that we have now. It is considered possible to navigate the existing privacy environment although this is not without some risk and may require future changes.” [8]. Hence, any policies that our data custodians follow need to be highly flexible and reviewed on a regular basis.

Health data can be used for many different purposes. This paper considers two case studies, one concerned with the implementation of community health information management, including clinical records, and the other with the integration of various existing databases of patient’s records to allow researchers to perform population based studies. Currently in Australia, this secondary use of data, in some circumstances, is explicitly permitted but is often viewed as a legal and ethical minefield. However, for medical researchers and health service providers it provides valuable information on things such as cause of the disease and best treatments or the patient journey and disease clusters. In order that research can continue to inform and improve Australians’ health while complying with the Privacy Act [9], the National Health and Medical Research Council [10] has issued guidelines approved by the Privacy Commissioner. Although this provides health researchers valuable access to data without patient consent, there are risks associated with the trust that individuals and data custodians have in keeping such data securely de-identified.

This paper considers the question of how application or organisationally dependent these risks are and, therefore, to what degree any risk management should be customised to suit. The case studies presented show that a risk based security analysis alone will not adequately address some of the key issues affecting trust and successful deployment. That is, different critical attributes have been identified in addition to security, that require their own evaluation methods and yet each attribute has an effect on the risks being addressed. The examples given emphasise that these attributes are not independent. This paper will, therefore, evaluate the benefit of using a risk based method that systematically investigates interdependencies between critical attributes. The key results from the case studies are presented, from which the need for further research is discussed.

2. The QUIPS model

The quality of a software product is an insufficient determinant to establish if it can be considered legally safe and secure. That is, a product may provide excellent reliability yet not have any features to protect from the particular hazards that a given working environment presents. This is well known in the safety-critical community whereby system-wide analysis

to include the operational and management aspects are incorporated into any hazard analysis. Security specialists are also aware of this requirement, although from our case study experiences it is evident a wide range of knowledge and capabilities are to be found within the Australian health industries when it comes to deploying effective IT security and safety measures, compounded by the patchwork of legislative requirements.

The QUIPS model [11] aims to provide a set of related methods that address the most pertinent issues facing the successful deployment of today’s electronic health systems. The model has been derived based on the experience of several research projects and consultancies using real e-health case studies undertaken by the authors [12–14]. The QUIPS model is based on the investigation of four critical attributes, namely *Quality, Usability, Privacy and Safety*. Other IT applications might prioritize things differently. In the software games industry, for example, Performance is a high priority whereas Safety would not normally be taken into consideration. Balancing such constraints, many of which conflict, is standard practice with software engineers. The QUIPS model provides a framework from which the interdependencies of these attributes can be assessed.

Code	Attribute	At risk
Q	Quality	i. Not developing the right product (i.e. not meeting requirements) ii. Not developing a robust product (i.e. not well engineered)
U	Usability	i. Degree of usage (i.e. full or partial use of functions) ii. Acceptance by users (e.g. clinicians, patients, administrators)
P	Privacy	i. System security (i.e. preventing unauthorised access) ii. Patient confidentiality (e.g. not revealing personal health data)
S	Safety	i. Harm to the system (e.g. availability, data corruption) ii. Harm to people (e.g. medical errors, medical data integrity)

For example, with Emergency Services poor IT usability could present a high risk. A risk based hazard or incident analysis would not determine the usability of a system for which a separate and specific evaluation is required. QUIPS provides a wider framework for investigating the attributes their social and technical aspects and a systematic approach to handle their interdependencies.

2.1. Case study—CHIME

CHIME is a Community Health Information Management Enterprise system implemented in New South Wales Health, Australia [12]. It is an operational, clinical information system that is designed to improve service delivery, outcome measures and productivity, through improved capture and man-

agement of Community Based Health Service Information. Staff are able to do a variety of functions more easily including accurate documentation of client assessment, develop individualised management plans based on best practise principles, monitor outcomes of clinical care and generate reports for client and management. CHIME was first implemented in the Child Assessment Intervention Team (CAIT) in November 2002 and then in the Aged Care Assessment Team (ACAT) in July 2003. At the request of the CHIME management team the authors initially undertook a usability analysis [12,14] followed by a safety analysis [13].

Usability Evaluation of CHIME began just before the implementation at CAIT and continued with the implementation at ACAT. The clinicians in CAIT and ACAT practise a wide variety of health services ranging from psychologists, speech pathologists, audiologists, occupational therapists, physiotherapists, dementia specialists and nurse clinicians. There were 21 clinicians from CAIT and 9 clinicians from ACAT who took part in this research. The approach taken involved a variety of methods, including semi-structured interviews, questionnaires and recording of actual usage on the system using Camtasia software for voice and screen capture. This was conducted at several stages of the implementation; before CHIME was implemented, after the clinicians were trained and after 3 months' usage. The three attributes of usability, i.e. *efficiency, effectiveness and satisfaction*, were evaluated by collecting usability metrics. An expert heuristic evaluation of CHIME's usability involving 372 questions was also carried out. Heuristic evaluation involves having a small set of evaluators examine the interface and judge its compliance with recognized usability principles (the heuristics). These heuristics refer to various aspects of a system, ranging from its visibility, error prevention, design, and user interaction.

The safety analysis was conducted after the system implementation. This involved a team of experts from the CHIME management team, health and safety officials and clinical experts in management positions. A fault tree of all prior and

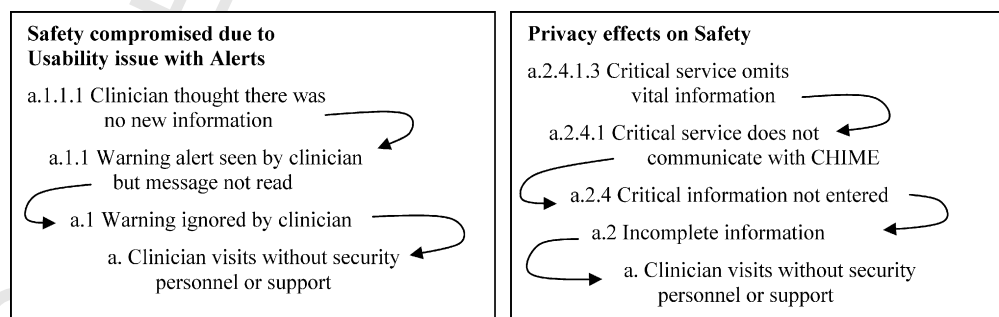
undertaking 20 related projects. The primary goal is to improve our knowledge in the area of preventative health to save \$2 billion in direct costs in Australian health care provision for chronic diseases. HDI™ has the capacity to provide unique insight into possible causes and effective prevention methods through extensive population studies of collected health data. This data is dispersed across several data bases with many custodians responsible for its integrity and privacy. Note this data is located in several states each with their own legal requirements relating to data handling sharing and security to meet their own individual interpretation of the National privacy legislation.

The architecture of HDI™ is being developed to provide state-of-the-art in robust security technology and flexible access control mechanisms. This has to be coupled with the privacy requirements to limit the movement and access of identifiable data yet at the same time permit matching of records to facilitate research. In the handling of sensitive information, Trust is a critical factor that can take years to build and a moment to break. The successful outcome of HDI™ and p-Health relies on building and maintaining such trust against a backdrop of shifting policies on data protection.

3. Applying QUiPS to evaluate e-health safety and security

3.1. Interdependencies with CHIME

One of the powerful features of the QUiPS model is in the identification of interdependencies between the critical attributes. Having identified some of the root causes that could lead to a safety incident, what roles do the usability and privacy of the system play in this? For example, from one of the identified hazards where the 'clinician visits without security personnel or support' [13], it can be seen how both privacy and usability issues that arise directly from the introduction of IT systems, could compromise safety, as follows:



perceived incidences were charted against which estimates of likelihood of occurrences was incorporated.

2.2. Case study—health data integration

Within the Australian's Commonwealth research agency (CSIRO) integration of health data is being supported by HDI™ [15]. This is a powerful software tool that underpins the linkage of critical information across disparate database sources. It is used by the CSIRO's Preventative Health (p-Health) Flagship program [16] involving over 100 researchers

From the usability evaluations, CHIME was considered highly usable [12]. That is both from the system design perspective and from some of the end-user's perspective. Not all users accepted the system and this had an effect on their perception of CHIME's usability. No matter what you do some users will determine that a system is totally unusable and non productive for cultural and political reasons, as evident in [12]. User acceptance is not one of the attributes associated with usability (see above). The QUiPS model helps identify this shortcoming as a potential risk prompting the adoption of acceptance testing using TAM [14]. As with any health

information system incorrect use could put both patients and clinicians at risk.

From the initial safety analysis [13] no high risk safety issues were evident that came from the implementation of an IT system. From the management's perspective the main safety concerns would come from ensuring all users are sufficiently knowledgeable on the capabilities and content of the CHIME system. Incorrect assumptions about the type and use of data contained by CHIME could present a higher than acceptable risk, for example, the completeness of information about a patient who has been transferred from other clinics or private hospitals. Users who become complacent are another concern, for example, ignoring alerts or leaving live data accessible during training sessions. Privacy was paramount from the management perspective but difficult to implement in a widely acceptable manner. The analysis to date has shown that all the critical characteristics had demonstrable interdependencies. Using QUiPS ensured that the safety and security can be minimised to acceptable levels without compromising the usability or privacy requirements, which is essential for ensuring successful adoption of a system deployed in the sensitive health care sector.

3.2. Consequences of health data integration

In consultation with the practitioners, a number of consequences have been derived that could arise from incidents occurring. Incidents may manifest in various ways, for example, inappropriate publication of results, letters sent out to the wrong people or media involvement with an alleged complaint. The consequences from incidents arising include:

- data not being supplied by patients/custodians;
- patients offended and taking legal action;
- research projects rejected by ethics committees;
- screening and prevention programs halted;
- loss of reputation and/or income;
- medical knowledge not advanced;
- incorrect treatment administered;
- collapse of our health care provision (particularly in disaster response situations).

For HDI™, our research is focusing is on providing, in addition to risk assessment, IT tools that assist in ascertaining the end users' knowledge, to check on their intended usage, to map against Federal/State legislation and local policies, to check on their ethics clearances and to enforce deadlines, audits and reviews. Our aim is to ensure such a process is always undertaken before permitting access to the data and data linkage tools. This will reassure the public, media and management that: the risks have been assessed, the probability of an incident has been estimated and adequate security and protection mechanisms have been put in place.

3.3. The risks with HDI™

Integrating health data across a number of disparate databases integration raises several questions:

- What are the new risks that health data integration brings?
- What techniques would quantify and minimize these risks?
- Do the privacy guidelines and legislation help or hinder?
- Can we realistically look at health care provision as a whole?
- What role does Trust play?

To address this, research undertaken with the Preventative Health Flagship has looked at the risks from differing viewpoints. That is, the management of data by the data custodians of the various health data bases across five states and the patients themselves (as the source of data).

This study has identified that the main risks as seen by the data custodians include:

- the accidental disclosure of individuals (M);
- contacting the wrong people, i.e. data records linking to the wrong people or the wrong reasons (VH);
- the incorrect use of data or for the wrong project or purpose (M → H);
- not having sufficient knowledge or control over their own data, i.e. in hands of IT services or third party (M → H);
- other data custodians not providing them data for linkage (H);
- not following the privacy principles and their local policies, i.e. as determined by ethics committees (L → M).

Five custodians have been involved in the study to date. The initial analysis shows the estimate of risk from low (L) through medium (M) to high (H) with the second risk showing as very high (VH) due to the incidences already experienced in this category. The preliminary study, which was based on interviews, will be expanded in 2006 for further detailed analysis of the two highest risk groups.

Whereas, this study has identified that the main risks as perceived by the public include:

- abuse of genetic data (e.g. disclosure to insurance companies);
- release of sensitive information (e.g. sexual, mental health);
- government control of personal data (including concern over using health identifiers as a national identity scheme since IDs are not a current Australian requirement);
- use of data without an individual giving explicit consent (primarily for research purposes);
- poor data integrity (information inaccurately recorded or records mismatched);
- inadequate safeguards (any access by unauthorised people).

The source of the data for assessing the public's perception has been mainly derived from the data custodians, the practicing clinicians and other related reports, e.g. a nationwide telephone study with a total of 1507 adults, see [17]. The practitioners are in constant contact with the public who have provided specific information on colorectal and lung cancer consisting of over 5000 patient records. Although many of these risks are perceived rather than based on actual or even probable incidences, the QUiPS analysis to date has highlighted how they could have a direct effect on the consequences. This has prompted further research to accommodate the perceived risk which is not adequately addressed with cur-

rent methods. That is, the current assumption that revised work practice and education can bring about effective change to minimised such risks is unfounded in practice, see [18].

4. Conclusions

Health data spans across numerous databases and jurisdictional boundaries. Hence, within Australia there is a need for joint agreement on the business process utilised such that any technical solution adopted will need to be driven by these processes and yet flexible enough to suit the differences at organizational, state and federal levels. Today's technology can provide a range of options for providing low risk solutions in the adoption of electronic health records. The biggest risk faced is in understanding the complex environments that our health services present and ensuring the users appreciate and comply with any policies set. Numerous divergent approaches continue to be researched aiming to provide practical, secure and compliant solutions that protect health data privacy. Convergence towards a viable universal solution is not imminent therefore trust in e-health is decidedly more fragile as compared with many other industry sectors. Hence, any policies that data custodians follow need to be flexible and updated on a regular basis to allow for changes.

The case studies presented, although within the Australian context, indicate that the methods used to derive the requirements are often inadequate. The risks that are faced in ensuring a safe and secure system are highly application dependent. Furthermore, with the constant changes in system interconnectivity against a backdrop of changes in legislation these risks are high dynamic. It is evident that the current conventional approaches taken are incapable of determining or facilitating an ongoing low risk solution. That is, from a security perspective, the technological solutions are at best a stop gap to avoid the common hazards associated with access control and secure messaging. A wider range of analysis techniques to determine the key issues for a dependable health information system, as presented in this paper, is proposed as a more comprehensive method for deriving solutions that are sustainable in the longer term.

Summary points

What has been learnt from this research?

Prior to undertaking this research the knowledge of the risks associated with the use of electronic health data was not sufficiently well understood within the context of the applications for the case studies selected. Since risk is a derivative of the consequences (that result from failures) they are highly application dependent. Some attributes of applications can be generalised permitting effective protective measures from known hazards, for example, the need to encrypt messages to reduce the risks associated with interception. To rely entirely on this approach can result in some significant high level risks remaining, particularly when they relate to the specific usage and implementations. Furthermore, unforeseen incidences are often associated with complex interdependencies between competing features and functions.

The result of this research has increased our knowledge of some of the interdependencies and how a structured method can be used to identify them effectively. A further finding has been that the risks derived from calculation based on past incidences and prediction by experts significantly deviates from the perceived risks associated with our primary data source, i.e. the patients. This is significant in that it indicates how we should modify or expand our methods to accommodate these perceived risks which are putting the opportunity to undertake future medical research at high risk. This is an area of national significance where preventative health programs require knowledge for effective diagnostics, treatments and protective foods.

REFERENCES

- [1] Common Criteria, Common Criteria for Information Technology Security Evaluation, August 2005, Version 2.3. <http://www.commoncriteriportal.org/> (accessed December 2005).
- [2] G. Bleumer, Introduction to the SEISMED Guidelines; The SEISMED Consortium (eds.), SHTI vol. 31–33, Data Security for Health Care, vol. I–III, IOS Press, Amsterdam, ISBN 9051992637, 1996, pp. 1–10.
- [3] B. Barber, G. Bleumer, J. Davey, K. Louwerse, How to achieve secure environments for information systems in medicine, in: MEDINFO 95, Proc. Part 1, Int. Medical Informatics Assoc. (IMIA), Edmond, Canada, 1995, ISBN 0969741413, pp. 635–639.
- [4] B. Barber, K. Louwerse, J. Davey, White Paper on Health Care Information Security, Implementing Secure Healthcare Telematics Applications in Europe, September 1997. <http://www.ishtar.org.uk/> (accessed November 2005).
- [5] Rebecca T. Mercuri, The HIPAA-potamus in Health Care Data Security, *Commun. ACM* 47 (7) (2004) 25–28.
- [6] Habtamu Abie, Risk Analysis, Risk Assessment, Risk Management, 2005. <http://www.nr.no/~abie/RiskAnalysis.htm> (accessed December 2005).
- [7] Health Connect, Fact Sheet—HealthConnect, 2004. <http://www.healthconnect.gov.au/about/Fact.htm> (accessed September 2005).
- [8] NEHTA, The National E-Health Transition Authority, 2005. www.nehta.gov.au (accessed September 2005).
- [9] Privacy Amendment (Private Sector) Act, 2000. <http://www.privacy.gov.au/publications/> (accessed September 2005).
- [10] NHMRC, Guidelines (s.95 and s.95A), Under Section 95 of the Privacy Act 1988, Published by National Health and Medical Research Council, Reference No: E26, 2000.
- [11] P.R. Croll, J. Croll, Q.U.i.P.S. a quality model for investigating risk exposure in e-health systems, *Medinfo J-2004* (2004) 1023–1027 (ISSN: 1569-6332).
- [12] J. Croll, P.R. Croll, The system versus the user: an evaluation of CHIME from two different perspectives, in: Proc.12th National Australian Health Informatics Conference HIC2004, Brisbane, 2004, ISBN 0 9751013 1 5.
- [13] P.R. Croll, J. Croll, Quality assurance of electronic health information systems using QUIPS, in: Health Informatics Conference Melbourne, HIC 05, August 2005.

- 390 [14] P.R. Croll, J. Croll, Usability evaluations in community health 399
391 systems, in: The International Conference on Qualitative 400
392 Research, QualIT 2004, Australia, November 2004. 401
- 393 [15] D.P. Hanson, C. Daly, K. Harrap, J. Jacquet, M.A. O'Dwyer, C. 402
394 Pang, J. Ryan-Brown, Health data integration: research 403
395 software to commercial product, in: Australian Software 404
396 Engineering Conference, ASWEC 05, Brisbane, April 2005. 405
- 397 [16] Preventative Health Flagship, Improving the health and 406
398 wellbeing of Australians through research into prevention, 407
early detection and intervention, Commonwealth Scientific 408
and Industrial Research Organisation, 2005. 399
<http://www.csiro.au/> (accessed December 2005). 400
- [17] R. Morgan, Community Attitudes Towards Privacy, Report 401
Prepared for The Office of the Federal Privacy Commissioner, 402
Roy Morgan Research, Sydney, Australia, 18 June 2004. 403
- [18] P.R. Croll, H. Morarji, Perceived risk: human factors affecting 404
ICT of critical infrastructure, Proc. Research Network for a 405
Secure Australia (RNSA) Conf. on The Social Implications of 406
Information Security Measure on Citizens and Business, 407
Univ. Wollongong, Australia, ~~29th May 2006~~, ~~in press~~. 408

UNCORRECTED PROOF