1-1-2012

Legal Issues Related to Accountable-eHealth Systems in Australia

Randike Gajanayake

Bill Lane
Queensland University of Technology

Tony Iannella
Queensland University of Technology

Tony Sahama
Queensland University of Technology

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

LEGAL ISSUES RELATED TO ACCOUNTABLE-EHEALTH SYSTEMS IN AUSTRALIA

Randike Gajanayake[1], Bill Lane[1, 2], Renato Iannella[1, 3] and Tony Sahama[1,4]
[1]Science and Engineering Faculty, Queensland University of Technology
[2]Clayton Utz
[3]NEHTA
[1]g.gajanayake@qut.edu.au, [2]wb.lane@qut.edu.au, [3]renato.iannella@nehta.gov.au, [4]t.sahama@qut.edu.au

Abstract
Information privacy requirements of patients and information requirements of healthcare providers (HCP) are competing concerns. Reaching a balance between these requirements have proven difficult but is crucial for the success of eHealth systems. The traditional approaches to information management have been preventive measures which either allow or deny access to information. We believe that this approach is inappropriate for a domain such as healthcare. We contend that introducing information accountability (IA) to eHealth systems can reach the aforementioned balance without the need for rigid information control. IA is a fairly new concept to computer science, hence, there are no unambiguously accepted principles as yet. However, the concept delivers promising advantages to information management in a robust manner. Accountable-eHealth (AeH) systems are eHealth systems which use IA principles as the measure for privacy and information management. AeH systems face three main impediments; technological, social and ethical and legal. In this paper, we present the AeH model and focus on the legal aspects of AeH systems in Australia. We investigate current legislation available in Australia regarding health information management and identify future legal requirements if AeH systems are to be implemented in Australia.

Keywords
eHealth, information privacy, information accountability, accountable-eHealth, privacy law, data breach, legal issues, legislation

INTRODUCTION
Australia's eHealth landscape is developing rapidly. Central to the Australian eHealth system is the timely availability of accurate health information. The availability of patient health information to the correct healthcare provider (HCP) is a significant issue. Poor availability of patient information can leads to serious medication and medical errors (Williams, 2011). But making patient data more available however, raise concerns with regards to information privacy. Information privacy centres on the regulation of personal information and is therefore a complicated issue in relation to healthcare information. This is because privacy requirements of patients and information requirements of HCPs are two competing concerns, and reaching an appropriate balance has proven difficult. Although information privacy definitions vary in healthcare information privacy literature (Parks, Chu, & Xu, 2011), the prominent definition still implies a sense of control of information by the owner or the subject (Westin, 1967). But in a specialised domain such as healthcare, relegating the control of health information to the patient is somewhat questionable. Therefore, a shared ownership between a patient and an entity with the appropriate domain knowledge must be sought in order to reach the aforementioned balance of requirements.
Controlling how authorised entities (e.g. HCPs) use information is another sensitive aspect. Most available measures addressing this issue such as access control are preventive measures that either allow or deny access to information, yet these preventive measures are inadequate to meet the requirements of the healthcare domain (Gajanayake, Iannella, & Sahama, 2012). We believe that by adhering to information accountability (IA) principles the aforementioned balance of requirements can be reached, and appropriate-use of health information can be enforced.
IA is a comparatively new concept to computer science and to the electronic society (Weitzner *et al*., 2008). It is where the consumers of information are held answerable for their actions and the ramifications of those actions. Information systems which adhere to IA principles are called accountable-systems and in an eHealth setting, this gives rise to 'Accountable-eHealth' (AeH) systems. AeH systems face three main impediments; technological, social and legal. In this paper, we focus on the legal issues of AeH systems in Australia. We investigate current legislation available in Australia regarding health information management and identify future legal requirements for AeH systems to be implemented in Australia.

LEGAL ISSUES RELATING TO HEALTH INFORMATION MANAGEMENT

The developing eHealth landscape raises a number of important legal challenges, particularly in relation to the establishment of an effective system for sharing eHealth records. The two principal areas of legal relevance are, firstly, the law of information privacy - especially within the realm of sensitive information such as health information and secondly, the appropriate governance and regulatory mechanisms necessary to manage, monitor and control the system established to provide for shared eHealth information.

Australian information privacy law

Measures relating to the protection of information privacy at the federal level are set forth in the 'Privacy Act 1988' (Cth) ("Privacy Act", 1988), which establishes a comprehensive statutory scheme based on 11 Information Privacy Principles (IPPs) and 10 National Privacy Principles (NPPs) which govern the retrieval, compilation, storage and use of personal information by federal government agencies and private sector organisations respectively. Under the Act, 'health information' forms part of a subset of personal information defined as 'sensitive information' - which is given a higher level of protection under the NPPs (but not the IPPs). IPP/NPP 4 contains the fundamental "Information/data security" obligation which requires agencies and organisations to take reasonable steps to secure personal information. Monitoring and compliance functions under the Act are undertaken by the Office of the Australian Information Commissioner (OAIC).

Measures of protection provided under the 'Privacy Act 1988' (Cth) are essentially limited to federal government agencies and private sector organisations. At the same time, various forms of statutory and non statutory measures exist at the State and Territory level for the protection of information privacy. This has resulted in a somewhat complex web of overlapping and inconsistent provisions inimical to the development of a comprehensive and uniform national regime of protection and control.

A nationally consistent approach to information privacy and health information management in particular is therefore vital and to that extent, the Commonwealth government's acceptance of recommendations contained in a report by the Australian Law Reform Commission (ALRC) 'For Your Information: Australian Privacy Law and Practice' (Australian Law Reform Commission, 2008) promises to achieve this. Major amendments to the 'Privacy Act 1988' (Cth) are now imminent, aimed at achieving national consistency in information privacy protection. The principal change will bring the IPPs and NPPS together to create one uniform set of Australian Privacy Principles (APPs), ensuring in the process that additional protections exist for health information (as a category of sensitive information) regardless of whether it is held by government agencies or private sector organisations.

More specifically in relation to eHealth, the 'Personally Controlled Electronic Health Record Act 2012' (Cth.) (PCEHR) ("Personally Controlled Electronic Health Records Act 2012", 2012) contains provisions which link that legislation with the privacy protection measures contained in the 'Privacy Act 1988' (Cth.). In this respect, the OAIC becomes the independent regulator of the privacy and personal data protection issues arising in relation to the regime established for eHealth information sharing by the PCEHR.

Regulation of the ehealth sharing regime

As indicated earlier, the second area of legal relevance concerns the need to ensure that appropriate governance and regulatory mechanisms exist to oversee, monitor and manage the eHealth sharing regime. Following the development of a number of electronic health information systems across Australia, the National E-Health Transition Authority (NEHTA) was established in 2005 as a joint initiative by the Australian, State and Territory governments. NEHTA's charter included setting national standards for the electronic collection and exchange of health information and encompassed the design of a system for Shared Electronic Health Records (SEHRs) based on the development of Unique Healthcare Identifiers (UHIs).

ALRC Report No 108 of 2008, referred to earlier, advised that the establishment of a national SEHR scheme would required the development of sufficient oversight and regulatory controls sufficient to ensure public trust and confidence in the system. Reference was made earlier to the enhanced role to be undertaken by the OAIC in relation to privacy protection arising in relation to the PCEHR. In addition to this, the OAIC will have the role of receiving and inquiring into data breaches which arise as a result of the operation of the PCEHR which the relevant entities are obliged to report. At a broader level of regulation, the PCEHR also establishes a number of entities with specific advisory and monitoring functions, including the Jurisdictional Advisory Committee and the Independent Advisory Council. The jurisdictional advisory committee is responsible for advising the system operator of the PCEHR system on matters relating to the interests of the Commonwealth, States and Territories where as the independent advisory council has the function of advising the system operator on the operation of the PCEHR system, participation of the PCEHR system, clinical, privacy and security matters relating to the operation of the PCEHR system and similar matters set down by the regulations ("Personally Controlled Electronic Health Records Act 2012", 2012).

ACCOUNTABLE-EHEALTH SYSTEMS

Accountable-systems implement appropriate-use of information entailed by accountability in terms of (legal) penalties. Their goal is to be non-restrictive in terms of information availability to legitimate users.

Accountability systems provide incentives to the users to implement this appropriate use of information. The underlying idea is that when users are aware of accountability mechanisms in place, they would deter from engaging in inappropriate system activities. Thus, allowing information to be made available for the legitimate users more openly and effectively. The knowledge of the existence of accountability mechanisms acts as an incentive towards increasing the trust of information owners.

An overview of the accountable-ehealth model

In the AeH model, HCPs are subject to information usage policies set by information owners/subjects. But, given the contextual nature of the domain, HCPs are allowed to use information for purposes they see appropriate which may be outside of the said policies but are justifiable given the circumstances or other domain constraints. Such systems enforce transparency such that all relevant consumers are aware of the operations done within the system. When a patient is notified of a breach of policy, she can choose to make an inquiry as to why her health information was used in such a manner. The HCP in question must then justify why the information was used in such away. The AeH model is shown in Figure 1.

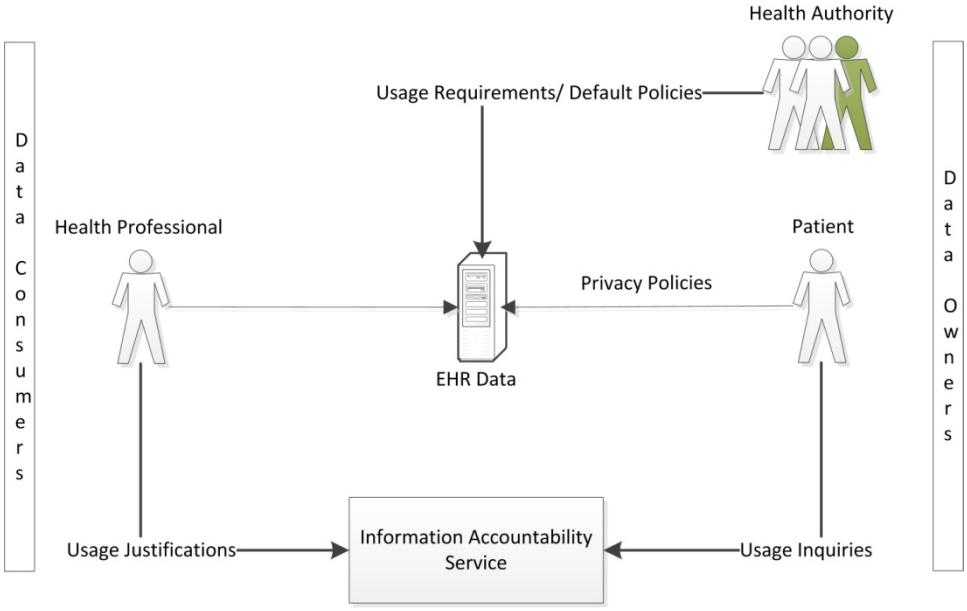

Figure 1: Accountable-eHealth Model (Gajanayake, Iannella, Lane, & Sahama, 2012)

We present the following characteristics of AeH systems.

- **Information control**: AeH systems extend some control of information to the patients. But given the nature of the industry, patients' privacy requirements can only be satisfied within boundaries which do not overlap with adequate healthcare delivery.
- **Information access and usage**: HCPs access and use health information to make decisions towards delivering appropriate healthcare for the patients. How they use health information is controlled by predefined policies.
- **Notification**: To enforce transparency, AeH systems propose a notification process where all participants are kept informed about the policies and the activities of the system. In this process the HCPs are notified of actions (access to information) that are outside of their allowed capabilities and patients are informed of possible misuse of their health information by HCPs. This would enable patients to be aware of how their health information is being used and HCPs to be more alert towards inadvertently accessing the wrong information.
- **Inquiries and Justifications**: In circumstances where possible misuse has occurred, the patients are given the capability to make inquiries directly to the HCP. The HCP is obligated to justify his actions. Providing this capability to the patients enable AeH systems to be more open and patient centric.
- **Provenance**: Provenance of electronic data deals with the history or a record of transactions performed on a data object. A record of such would enable computer systems to reason over the life cycle of a data object. A clear record of all user activities is crucial for AeH systems. To facilitate this, policy-aware transaction logs are maintained in AeH systems for the purpose of validation of the justifications by HCPs to patient inquiries and to facilitate transparency.
- **Penalties and redress**: Adequate measures must exist to minimise the extent of negligent or intentional misuse of health information by an HCP. Such measures should ideally be designed to

operate as both a deterrent against such behaviour as well as an incentive for HCPs to act appropriately, given the sensitive nature of the relevant information.

LEGAL ISSUES RELATED TO ACCOUNTABLE-EHEALTH SYSTEMS

Data ownership and patient control of health information

Protecting the public's interest through legislative reform and ensuring people retain control over who has access to their personal health information in crucial (OAIC, 2008). According to Australian federal legislation, health information is generally owned by the HCP who creates and manages the data. But despite this ownership by HCPs, patients retain the right to access their health records. These laws do not cover the full extent of data ownership and the information control issues with regards to health information. However, in light of the newly enacted PCEHR Act, patients can define access control settings for all their clinical documents and nominate HCPs who can access them. This offers a certain degree of ownership to the patients similar to what is required by AeH systems.

Access and use of health information

The ALRC recommends a nationally consistent policy for handling health information (Australian Law Reform Commission, 2008). In the PCEHR Act, a definition of the use and disclosure of health information in a consumer's PCEHR is given which states that the users (including HCPs) of the PCEHR system should adhere to the access controls set by the registered consumer (patient) at all times when collecting, using and disclosing health information except in some circumstances as stated in the Act ("Personally Controlled Electronic Health Records Act 2012", 2012). Use and disclosure of health information (mostly health identifiers) is also handled by parts of the 'Health Identifiers Act 2010' ("Healthcare Identifiers Act", 2010).

The most significant aspect of AeH systems is that health information is made available to the relevant HCP without rigid access restrictions. They also recognise explicit purposes for which data can be accessed. Even though an underlying access policy exists, an HCP is allowed to override the existing policy given his professional role. But intentional misuse is entailed by punishment which acts as an incentive not to misuse health information. Hence AeH systems require laws which explicitly define how electronic health information should be accessed and used by HCPs.

Data breach notification

Data breach notification is crucial for AeH systems, since consumer trust is gained through transparency which entails that all participants are kept well informed of how information is managed. The concept of data breach takes its focus from events such as computer hacking, theft of storage equipment, the inadvertent publication of personal information and the improper decommissioning of storage equipment. However, misuse of personal information by organizational employees can also be considered a form of data breach (Burdon, Lane, & von Nessen, 2010; Kierkegaard, 2011).

Data breach notification plays a significant role in relation to information privacy law since information subjects, with certain degree of control of their information, clearly deserve the right to be informed about breaches of their personal information – particularly those occurring within specific settings such as healthcare. In terms of data breach notification generally, the Australian Government, although aware of its significance, has not been as active as other jurisdictions such as those in the US and the EU. At this stage in Australia, there has been no enactment of a general statutory data breach notification law (Burdon, Lane, & von Nessen, 2012) although one now appears imminent (see below). In the meantime and in the absence of such a law, the OAIC re-issued voluntary notification guidelines to assist and encourage stakeholders to maintain appropriate security measures, report breaches and generally to promote a culture of notification (OAIC, 2012a).

In ALRC Report No 108 of 2008, the ALRC recommended an amendment to the 'Privacy Act 1988' (Cth),to create a statutory reporting obligation based on a two-stage notification trigger requiring, firstly a reasonable expectation that there has been an unauthorized acquisition of specified personal information (which would include both personal information and sensitive personal information - such as health information) and secondly, a real risk of serious harm as a result of such disclosure to an affected individual (Recommendation 51-1).

More recently and as part of its 2nd Stage Response to ALRC Report No 108 of 2008, the Australian Government finally released a Discussion Paper, 'Australian Privacy Breach Notification' (Commonwealth of Australia Attorney-General's Department, 2012) which announced the government's intention to legislate in response to the ALRC recommendation. The Paper outlines relevant issues and options with respect to the nature and wording of a mandatory data breach notification regime and invites submissions from the public.

Although the 'Privacy Act 1988' (Cth) has not yet been amended to include a general data breach notification obligation, the Australian government was prompt in establishing a specific mandatory data breach notification regime for eHealth information. This regime, set forth in the PCEHR Act, establishes a legal obligation to report data breaches in the circumstances set forth in the statute. To assist stakeholders in understanding and complying with their legal obligation to report data breaches under the PCEHR system, the OAIC has published draft guidelines, 'Mandatory Data Breach Notification in the eHealth Record System' (OAIC, 2012b).

Transaction logs

Provenance has been identified as a key characteristic of AeH systems. Information about how data is used by HCPs is crucial especially when validating justifications by HCPs. The transaction logs of one's own EHR must be accessible to the patients. It must be clearly stated in appropriate legislation how the logs are maintained and who, how and for what reasons they can be accessed and used. Currently, the PCEHR Act identifies the access to audit logs in the PCEHR system only as a system operator's obligation. The "PCEHR concept of operation" document however, contains detail of the consumers' rights to access audit logs (National E-Health Transition Authority, 2011). But we contend that in AeH systems (if not for the PCEHR system) the patients should also retain the right to access transaction logs in their own EHR and must be formally established through legislation.

Resolving disputes

A consumer (patient) of an AeH system is entitled to make inquiries pertaining to certain usage of their health information by a HCP which the system determines that could be potentially harmful to the consumer. The HCP in question is required to make a valid justification of his or her use of the consumers' health information. It is the invalid justifications that are followed by legal penalties. The PCEHR Act defines several scenarios where participants (including HCPs) of the PCEHR system can collect, use and disclose health information outside of the access controls set by the consumers. But these scenarios are mostly for special circumstances and do not cover general use of health information, and in turn, do not cover what is required by AeH systems.

In the case of a dispute between a patient and an HCP relating to inappropriate use of health information, a defined method for resolving that dispute is required. Unlike cases of medical negligence, which are already addressed by law, resolving disputes relating to health information usage are not well defined within the legal framework. A clear definition of legal penalties for misuse of information is required for AeH systems because they rely heavily on deterrence trough incentives. The penalties must be unambiguously defined and expressed such that they are well understood by all participants of the system. However, without covering all other aspects relates to intentional data breaches, the definition of these penalties is unlikely.

As mentioned earlier, AeH systems define a protocol for inquiries and justifications for potential misuse of information. This acts as the initial dispute resolution protocol. Issues can be resolved if a justification given by an HCP is deemed valid by the system and if the patients concur. But there are no AeH explicit protocols defined for situations where HCPs fail to provide a valid justification. Although the AeH protocols give some incentive (in the form of transparency) for HCPs to abide by usage policies, the yet undefined penalty measures are the real accountability measures that would deter HCPs from intentionally misusing health information at the same time increase patient confidence in sharing their health information with HCPs.

DISCUSSION AND CONCLUSION

AeH systems are meant to address the privacy conundrum by balancing competing concerns of healthcare stakeholders. Although AeH systems have not yet been fully implemented, they have the potential to operate as an effective countermeasure for privacy threats. We have demonstrated that adequate legislative foundations are critical for AeH systems. Yet at this stage, it would appear that the current Australian legal framework relating to health information management falls short of what is necessary and appropriate for the proper implementation of AeH systems.

Specifically, in order for AeH systems to operate effectively in the Australian context, a privacy breach protocol (Cavoukian, 2006) may be formulated that addresses AeH system characteristics and capabilities supported by existing and new legislation. Although some general guidance is provided by the recently updated 'Guide to Handling Personal Information Security Breaches' (OAIC, 2008) and the more specific 'Mandatory Data Breach Notification in the eHealth Record System' (OAIC, 2012b), there is currently no active and detailed privacy breach protocol in Australia. However, with the imminent enactment of a general data breach notification law, the foundations for developing such a protocol sufficient to underpin an AeH system are slowly being laid.

References

Australian Law Reform Commission. (2008). *For Your Information – Australian Privacy Law and Practice* (No. 108).

Burdon, M., Lane, B., & von Nessen, P. (2010). The mandatory notification of data breaches: Issues arising for Australian and EU legal developments. *Computer Law & Security Review*, *26*(2), 115-129.

Burdon, M., Lane, B., & von Nessen, P. (2012). Data breach notification law in the EU and Australia – Where to now? *Computer Law & Security Review*, *28*(3), 296-307.

Cavoukian, A. (2006). *What to do when faced with a privacy breach guidelines for the health sector*. Retrieved from http://hdl.handle.net/1873/1826

Commonwealth of Australia Attorney-General's Department. (2012). *Australian Privacy Breach Notification*. Retrieved from http://www.ag.gov.au/Consultationsreformsandreviews/Pages/Australian-Privacy-Breach-Notification.aspx

Gajanayake, R., Iannella, R., Lane, B., & Sahama, T. (2012). *Accountable-eHealth systems: The next step forward for privacy*. Paper presented at the 1st Australian eHealth Informatics and Security Conference (AeHIS) [*In press*].

Gajanayake, R., Iannella, R., & Sahama, T. (2012). *An Information Accountability Framework for Shared E-Health Policies*. Paper presented at the Workshop on Data Usage Management on the Web.

Healthcare Identifiers Act. (2010). Retrieved from http://www.comlaw.gov.au/Details/C2012C00590

Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review, 27*(5), 503-515.

National E-Health Transition Authority. (2011). Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. Retrieved from http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/PCEHRS-Intro-toc#.T9BeK8VIuSo

OAIC. (2008). *Guide to handling personal information security breaches*. Retrieved from http://www.privacy.gov.au/materials/types/guidelines/view/6478

OAIC. (2012a). *Data breach notification*. Retrieved from http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html

OAIC. (2012b). *Mandatory data breach notification in the eHealth record system*. Retrieved from http://www.oaic.gov.au/news/consultations/eHealth/mandatory_data_breach_notification_guide_draft_September2012.html

Parks, R., Chu, C.-H., & Xu, H. (2011). *Healthcare Information Privacy Research: Iusses, Gaps and What Next?* Paper presented at the Americas Conference on Information Systems. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1177&context=amcis2011_submissions

Personally Controlled Electronic Health Records Act 2012. (2012). Retrieved from http://www.comlaw.gov.au/Details/C2012A00063

Privacy Act. (1988). Retrieved from http://www.comlaw.gov.au/Series/C2004A03712

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Commun. ACM, 51*(6), 82-87.

Westin, A. (1967). *Privacy and Freedom*: New York: Atheneum.

Williams, P.A.H. (2011). Why Australia's health system will be a vulnerable national asset. In C. Valli (Ed.) *Proceedings of the 2nd International Cyber Resilience Conference*. pp. 99-100. Perth: secau- Security Research Centre, Edith Cowan University.