Edith Cowan University
Research Online

ECU Publications 2012

1-1-2012

# Accountable-eHealth Systems: the Next Step Forward for Privacy

Randike Gajanayake

Tony Iannella
*Queensland University of Technology*

Bill Lane
*Queensland University of Technology*

Tony Sahama
*Queensland University of Technology*

Follow this and additional works at: https://ro.ecu.edu.au/ecuworks2012

 Part of the Computer Sciences Commons

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
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks2012/99

# ACCOUNTABLE-EHEALTH SYSTEMS: THE NEXT STEP FORWARD FOR PRIVACY

Randike Gajanayake[1], Renato Iannella[1, 2], Bill Lane[3, 4] and Tony Sahama[1,5]
[1]Science and Engineering Faculty, Queensland University of Technology
[2]NEHTA [3]Faculty of Law, Queensland University of Technology
[4]Clayton Utz
[1]g.gajanayake@qut.edu.au, [2]renato.iannella@nehta.gov.au, [4]wb.lane@qut.edu.au, [5]t.sahama@qut.edu.au

## Abstract
*EHealth systems promise enviable benefits and capabilities for healthcare, yet the technologies that make these capabilities possible brings with them undesirable drawback such as information security related threats which need to be appropriately addressed. Lurking in these threats are patient privacy concerns. Resolving these privacy concerns have proven to be difficult since they often conflict with information requirements of healthcare providers. It is important to achieve a proper balance between these requirements. We believe that information accountability can achieve this balance. In this paper we introduce accountable-eHealth systems. We will discuss how our designed protocols can successfully address the aforementioned requirement. We will also compare characteristics of AeH systems with Australia's PCEHR system and identify similarities and highlight the differences and the impact those differences would have to the eHealth domain.*

### Keywords
eHealth, privacy, security, usage control, information accountability, PCEHR.

# INTRODUCTION
EHealth promise benefits to patient care through enhanced access to information and efficiencies in healthcare delivery (Scott, 2010). The World Health Organisation (2012) defines eHealth as 'the combined use of electronic communication and information technology in the health sector'. Considering current developments, this broad definition can be narrowed down to state that eHealth uses the Internet as the medium of communication allowing for an assortment of capabilities to be introduced to the healthcare domain. The nature of the Internet and that of the healthcare domain raises a number of concerns in regards to the security and integrity of the information. Health information is considered one of the most sensitive in any informatics domain (Cavoukian, 2006) thus, ensuring the security of the information is paramount for eHealth systems to be successful in delivering the capabilities it promises. But the medical environment has a poor history of uptake and implementation of security measures, as security has traditionally been seen as a business concept (Williams, 2007).

Electronic health records (EHR) are at the heart of eHealth (Ferreira, Shiu, & Baldwin, 2003). In health informatics literature, EHRs and electronic medical records (EMR) are often used synonymously. But there is a clear difference. EMRs are medical records of a patient created and maintained locally by a healthcare provider (HCP) whereas an EHR is a comprehensive medical records shared by all HCPs. Hence a patient may have more than one EMR but only one EHR. EHRs are a powerful tool for HCPs given this completeness and availability. EHRs are more beneficial than EMRs mainly because care givers are capable of accessing a patient's entire medical history rather than parts of it as with EMRs. An EHR system can be made available to care givers from anywhere where there is a suitable Internet facility. For example, HCPs can access it from their local practice, use all capabilities provided for them by the EHR system without having to invest in an expensive EMR system which can be a significant and costly investment for many practices (Yaffee, 2011). EHR systems however, bring with them their own risks.

Even with state-of-the-art security protocols put in place, there still remain issues related to patient privacy in terms of information use by authorised entities in the system such as HCPs. In this article we focus on information use by these authorised entities, more specifically HCPs, within the system whilst not addressing issues related to unauthorised access to the EHR system (e.g. hacking).

HCPs have a professional and ethical obligation to manipulate a patient's health information appropriately, i.e. use the information for the purpose of healthcare towards the benefit of the patient. With paper records, this ethical obligation goes a long way towards appropriate use of health information by HCPs. But there seem to be an intuition amongst eHealth stakeholders that information is susceptible to misuse when it is presented in an electronic form. The reason for this may be because information becomes more readily available and easily distributed in electronic form than when in a paper based form. This perception has lead to the increased

concern and focus on privacy issues related to health information. The access and use of paper records are governed by social norms (together with ethical practise) to an acceptable extent. But for EHRs it is not clear as to whether they have the same effect. EHRs are accessible from multiple locations unlike paper records which are kept in a single location. This freedom to access patients' health information, although hugely advantageous, eliminates some of the constraints which would deter consumers from misusing them. In a patient's point of view, this raises concerns as to whether their electronic health records are as secure as been claimed or whether they are vulnerable to abuse.

**A privacy conundrum**

As Goldman et al. states;

> "without trusting that their most sensitive health information will be safeguarded, patients are reticent to fully and honestly disclose their personal information and might avoid seeking care altogether" (Goldman & Hudson, 2000).

Therefore, increasing consumer trust in the system is critical for eHealth system success. The most significant impediment for the proliferation of eHealth systems is patient privacy concerns (Chen, Chang, & Wang, 2010).
Defining information privacy is difficult. The most widely accepted definition of privacy by Alan Westin states that

> "privacy is the claim of individuals, groups, or institutes to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967).

This definition implies a sense of control of information by the owners or subjects. Privacy concerns are usually coupled with information security which mainly involves unauthorised access by external entities. But addressing data breaches by authorised users pose the biggest challenge and it is a significant aspect for eHealth systems. Some even claim that privacy threats are internal factors and not external (Kierkegaard, 2011). Therefore, patients have an expectation of confidentiality in their dealings with any qualified clinician or HCP (Croll, 2011).
Access to information by internal users is controlled by preventive measures such as access control. But these are deemed unsuitable for a specialise domain such as healthcare. There is evidence to suggest that the lack of adequate patient information has given rise to serious medical errors (Williams, 2011) which threaten patient health. Therefore, the availability of timely, unrestricted and relevant patient health information to the appropriate HCPs is thus vital. Reaching a balance between information privacy requirements and the information requirements of patients and HCPs respectively is so elusive to healthcare policy makers as well as technology professionals. Reaching this Balance is centred on what we like to call 'appropriate use' of information. As regards to this in eHealth systems, we introduce the concept of information accountability (IA) and accountable-eHealth (AeH) systems.

## INFORMATION ACCOUNTABILITY AND ACCOUNTABLE-EHEALTH SYSTEMS

What is IA and what are AeH systems? IA is where the consumers of information are held answerable for their actions and the ramifications of those actions. EHealth systems which adhere to IA principles are therefore called AeH systems. As mentioned before controlling how authorised users use information is challenging. As regards to this, we have to raise the question; "*Will users only use data for the intended (or specified) purpose(s)?"* In a complex domain such as healthcare which is driven by specialised knowledge, controlling the usage of information by those specialists (HCPs) is somewhat a sensitive matter. It is not always the correct cause of action to impose restrictions to information access and usage on HCPs. But in terms of the privacy requirements of patients a certain degree of restriction to the usage is necessary.

### AeH systems

The goal of AeH systems is to be non-restrictive in terms of information availability to legitimate users. They provide incentives to the users to implement appropriate use of information. These incentives take the form of accountability entailed by penalties (Feigenbaum, Jaggard, & Wright, 2011). The underlying principle is that when users are aware that such use of information would lead to a negative outcome, they would deter from engaging in such activities. Thus, allowing information to be made available for the legitimate user more openly and effectively. In terms of the information owners' perspective, the knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives towards increasing their trust in the system.
The main conceptual principle of AeH systems is that when information consumers are aware of negative ramification towards them following inappropriate information use, they deter from engaging in such activities. This is more profound in the 'offline' world than in the 'online' world (Feigenbaum, Hendler, Jaggard, Weitzner, & Wright, 2011). This deterrence is governed by social norms that are accepted by the majority of the society. But it is not the case in the online world. Such norms are still in their embryonic stages and are not clearly defined nor widely accepted in the society. This creates problems for AeH systems. But it is the intention

that ones such systems become available and used by the majority of the community, the practices will become norms themselves.

**An overview of the accountable-ehealth model**

In our model we consider three types of users; a central health authority, patients, and HCPs. The health authority is the governing body responsible for managing the EHR system and managing its employees i.e. HCPs. The health authority defines default access levels for each HCP relevant to their role within the healthcare domain. The patients define their own access policies for the HCPs they nominate to give access to their health records according to individual privacy requirements. Using a predefined protocol, the two policies are combined such that the final operational policy assigned for each HCP satisfies both the patient's privacy requirements and the HCP's information requirements. HCPs who have been nominated by a patient to have access to his EHR will lodge usage requests containing the required data types and the intended purpose(s) for access. These requests are processed using a knowledgebase containing EHR data types and related purposes. All usage of EHR data by HCPs is stored as transaction logs for 'after-the-fact' accountability purposes. In an event of a possible misuse of a patient's health information by a HCP, the patient is capable of lodging an inquiry to the relevant HCP asking for a justification for his actions. The HCP is then required by the system to provide a valid justification for the particular usage. If the HCP fails to do so, he is held accountable for the ramifications of his actions. Figure 1 shows a simplified AeH model.

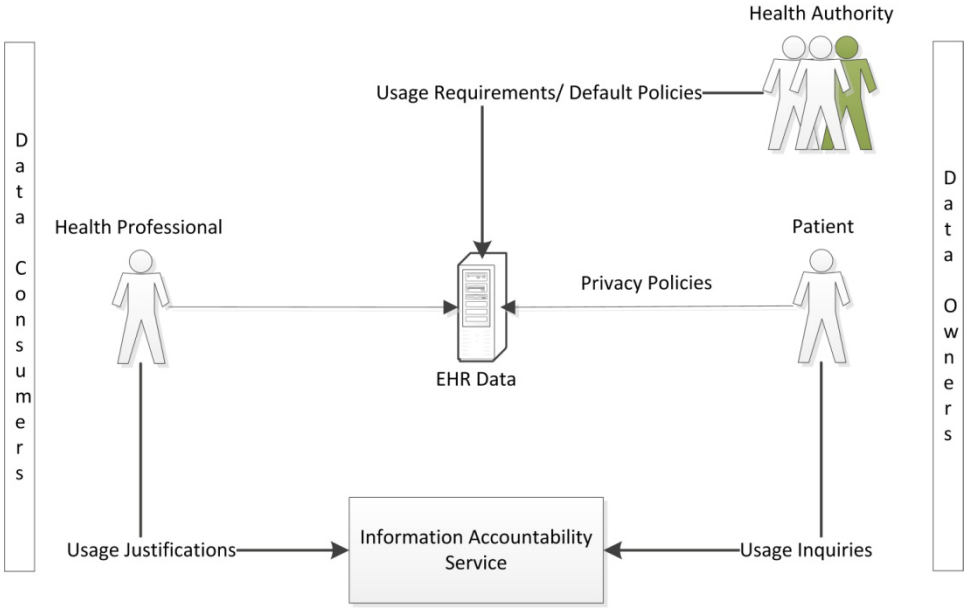


*Figure 1: Accountable-eHealth Model*

A detailed description of AeH system protocols and the accountability model is available in our previously published work (Gajanayake, Iannella, & Sahama, 2012a, 2012b). A simple use case diagram for the AeH model is shown in Figure 2.

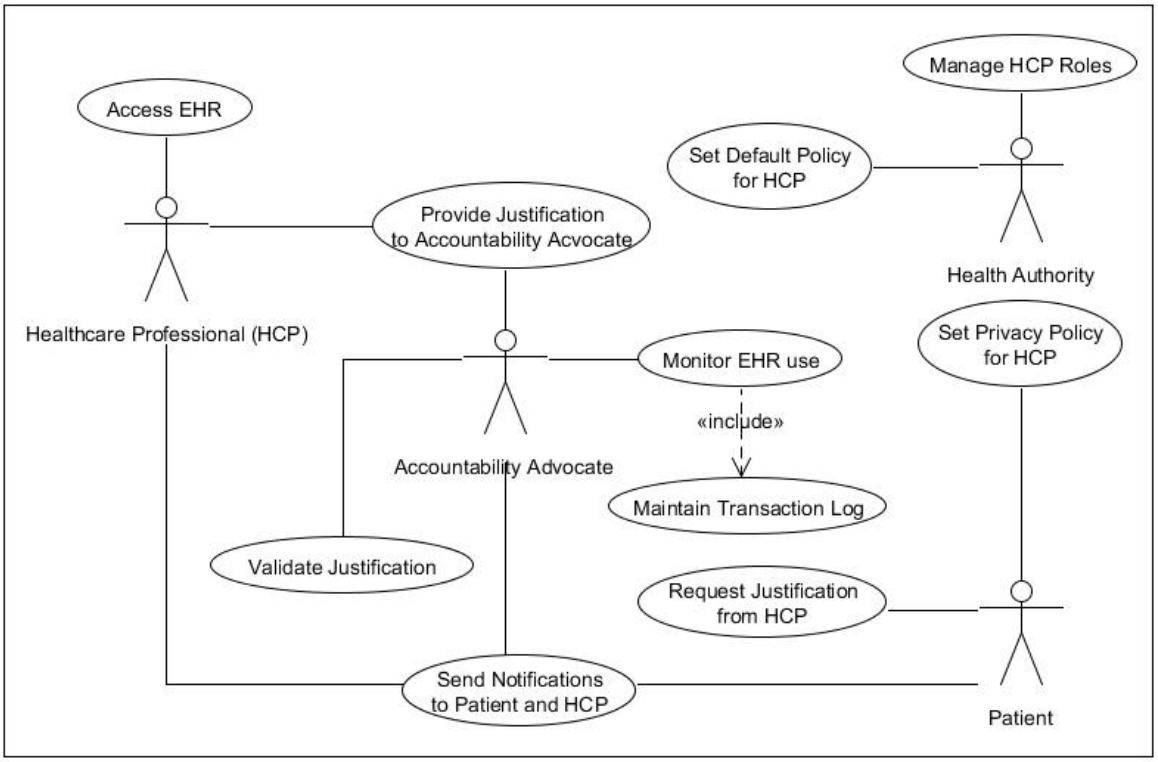


*Figure 2: Use case diagram for AeH systems*

**Characteristics of AeH systems**

In this section we will look at the characteristics and protocols of AeH systems designed towards meeting their goals.

**Control of health information**

Delegating control of personal information to the subjects has been seen as a means of addressing privacy in information sensitive domains. AeH systems extend control of health information to the patients as well as a governing health authority. This will ensure that fulfilling patient privacy requirements would not lead to a hindrance to healthcare delivery by HCPs. Policies for how information must be used are set either by the patients, a relevant authority or by both as seen in Figure 1. Patients nominate preferred HCPs to access information in their EHR. The HCPs are assigned specific levels of access as defined in the aforementioned policies.

**Information usage and justifications**

Health information must be used for the purpose of healthcare delivery for the patients. AeH systems require a comprehensive record of purposes for which information can be used by HCPs. These predefined purposes are maintained by the health authority. Although predefined policies govern the use of information in AeH systems, HCPs are allowed to access information that is outside of those policies to ensure that the required information is available to the HCPs in unforeseeable circumstances. This will however trigger an event in the system where the patient in question can request a justification for the use of information from the HCP. The HCP is obligated to justify his actions regarding the patient's health information. A patient may or may not choose to request a justification given the nature of the incident. Providing this capability to the patients enable AeH systems to be more open and patient centric. But it is also important to view this aspect in a HCP's perspective by considering their responsibilities towards providing quality healthcare to their patients.

**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.

**Provenance**

Provenance of electronic data deals with the history or a record of transactions performed on a data object. A record of the activities in the system must be kept in the form of policy-aware transaction logs which act as accountability information used to validate the above mentioned justifications by HCPs in the event of a conflict.

**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. These penalties must be communicated to the users such that they are aware of the consequences of intentional misuse of sensitive information.

## THE PCEHR SYSTEM AND AEH SYSTEMS

The Personally Controlled Electronic Health Record (PCEHR) system was launched in Australia on the 1st of July 2012 by the Department of Health and Ageing (DoHA) (National E-Health Transition Authority, 2011). Every Australian now has the chance to 'opt in' and create a shared EHR. The main aim of the PCEHR is sharing information or the creation of shared health summaries together with discharge summaries, event summaries, referrals, and consumer-based documents (e.g. consumer health summary). It enables the patients to enforce their own access control settings and select their preferred HCPs. Patients have the capability to 'opt out' at any point if they chose to. They also have the capability to remove documents from their EHR. These documents thereafter will not be visible to HCPs other than to the authoring healthcare provider organisation. Therefore, an HCP cannot make an informed decision just by looking at a patient's PCEHR. But with the capability to share EHRs nationwide easily makes the PCEHR system the most advantageous of its kind in Australia to date.

Similar to the PCEHR system, AeH systems allow patients to set access controls and usage polices to health information in their EHR. But in the policy formulation process AeH systems seek the involvement of a health authority. This ensures that relevant information is available to the caring HCP. So with AeH systems, the HCPs are capable of making well informed decisions by looking at the information accessible in the EHR. The policy overriding capability of AeH systems further ensures the availability of the information to the HCP. The PCEHR system also implements an override protocol for HCPs but it is only in the cases of emergency and circumstances where obtaining the consent of the patient is impractical. The accountability mechanism put in place in AeH systems allows patients to be more confident of the policy overriding process.

The PCEHR system maintains audits of system activities. PCEHR documentation states that the logs are accessible to the patients. Patient concerns over how an HCP has used their information can only be addressed through the PCEHR system operator. But AeH systems' inquiry and justification process allows patients to rectify matters directly with the HCPs. This process not only helps in conflict resolution but acts as an incentive for patients to increase their confidence on the security of their personal information. It must be noted however that this process should be carefully implemented such that HCPs are not overwhelmed by unnecessary inquiries by patients. The audit logs in AeH systems can be used in semantic reasoning such that justifications can be processed without the involvement of separate 'accountability advocates'. But if conflicts cannot be resolved via the available AeH protocol, the issues have to be escalated to a more comprehensive conflict resolution protocol which needs to be defined in an appropriate legal framework.

The establishment and operation of the PCEHR system is enabled by the PCEHR Act 2012 ("Personally Controlled Electronic Health Records Act 2012", 2012). Similarly, appropriate legislative foundations must be put in place is AeH systems are to be implemented in the future.

AeH systems are not an instant solution to the problems it seeks to address. EHealth systems need time to mature. For example, NEHTA believe that the PCEHR system would reach its full potential within the next 10 years. AeH systems also need time to mature.

## CONCLUSION

We have presented AeH systems which allow health information to be made more accessible to HCPs whilst ensuring the information is used appropriately. We argued that AeH systems are the answer for breaking eHealth free from the current privacy conundrum. In order for these systems to be effective in their venture, we contend that issues such as public awareness, ethical and professional conduct, and education and training (for both patients and HCPs) about the operation of AeH systems are important towards a successful implementation of AeH systems. It is also important that these systems be put through conformance system testing by third parties to ensure that they perform as intended. Accountable-systems in general have a long way to go towards achieving their goal of implementing appropriate use of information.

## REFERENCES


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.

Chen, K., Chang, Y.-C., & Wang, D.-W. (2010). Aspect-oriented design and implementation of adaptable access control for Electronic Medical Records. *International Journal of Medical Informatics, 79*(3), 181-203.

Croll, P. R. (2011). Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling. *International Journal of Medical Informatics, 80*(2), e32-e38.

Feigenbaum, J., Hendler, J., Jaggard, A. D., Weitzner, D. J., & Wright, R. N. (2011, 11 - 17 June 2011). *Accountability and Deterrence in Online Life.* Paper presented at the WebSci Conference 11, Koblenz, Germany.

Feigenbaum, J., Jaggard, A. D., & Wright, R. (2011). *Towards a Formal Model of Accountability*. Paper presented at the New Security Paradigms Workshop.

Ferreira, A., Shiu, S., & Baldwin, A. (2003, 26-27 June 2003). *Towards accountability for Electronic Patient Records.* Paper presented at the Computer-Based Medical Systems, 2003. Proceedings. 16th IEEE Symposium.

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

Gajanayake, R., Iannella, R., & Sahama, T. (2012b). *Privacy Oriented Access Control for Electronic Health Records*. Paper presented at the Workshop on Data Usage Management on the Web.

Goldman, J., & Hudson, Z. (2000). Virtually exposed: Privacy and e-health. *Health Affairs, 19*(6), 140.

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

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

Scott, J. (2010). The Impact of the E-Health (Personal Health Information Access and Protection of Privacy) Act. *Canadian Journal of Administrative Law and Practice, 23*(1), 55.

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

Williams, P. A. H. (2007). Medical insecurity: when one size does not fit all. In C. Valli and A. Woodward (Eds.), *Proceedings of the 5th Australian Information Security Management Conference*, 226-233, School of Computer and Information Science, Edith Cowan University, Perth, WA.

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.

World Health Organisation. (2012). eHealth at WHO. Retrieved from http://www.who.int/ehealth/about/en/

Yaffee, A. (2011). Financing the Pulp to Digital Phenomenon. *Journal of Health & Biomedical Law, 7*(2), 325-372.