Managing and sharing health data through Information Accountability protocols

Conference Paper · October 2015

DOI: 10.1109/HealthCom.2015.7454498

4 authors, including:

Tony Sahama
University of Victoria
120 PUBLICATIONS **1,312** CITATIONS

SEE PROFILE

Managing and Sharing Health Data through Information Accountability Protocols

Daniel Grunwell[1], Paulo Batista[2], Sergio Campos[2], and Tony Sahama[1]
[1]Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
Email: {d.grunwell,t.sahama}@qut.edu.au

[2]Department of Computer Science, Universidade Federal de Minas Gerais
Av. Antonio Carlos, 6627, Pampulha, 31270-010
Belo Horizonte, Brazil
Email: {paulo.batista,scampos}@dcc.ufmg.br

***Abstract*—Concerns over the security and privacy of patient information are one of the biggest hindrances to sharing health information and the wide adoption of eHealth systems. At present, there are competing requirements between healthcare consumers' (i.e. patients) requirements and healthcare professionals' (HCP) requirements. While consumers want control over their information, healthcare professionals want access to as much information as required in order to make well-informed decisions and provide quality care. In order to balance these requirements, the use of an Information Accountability Framework devised for eHealth systems has been proposed. In this paper, we take a step closer to the adoption of the Information Accountability protocols and demonstrate their functionality through an implementation in FluxMED, a customisable EHR system.**

***Keywords*—Access Control; electronic health records; EHR; eHealth; privacy; security.**

I. Introduction

Privacy is a critical but unfavourably defined concept, subjected to culturally dependent variables [1]. Privacy of an individual is breached when control over their personal information is lost to that individual [2]. eHealth systems and health service improvement are hindered by privacy concerns. The privacy and security of health information is a crucial factor in the success or failure of digital healthcare systems. The exposure of this information can cause significant repercussions to the individuals. At the same time, not having such information available when it is needed can lead to inaccurate decision making and avoidable and potentially life threatening clinical errors while providing clinical care. When protecting this information, both technical and human factors must be considered.

Many patients prefer the ability to control and restrict access to their health information; however, healthcare providers believe that patient's restricting access to their electronic health records (EHRs) would be detrimental to the quality of care [3]. This conflict between patient privacy desires, the needs of healthcare professionals (HCPs), and the quality of healthcare can be seen in the recent review of Australia's national Personally Controlled Electronic Health Record (PCEHR) system [4]. A balance must be found between these often competing concerns if such systems are to succeed.

Aiming to achieve this balance, we developed the Information Accountability Framework (IAF) [5], which provides the assurance of holding individuals accountable when health information exchanges take place. The IAF makes use of defined policies to determine appropriate use, with policies able to be defined based on types of data being accessed, the context of the information access (i.e. patient consultation), the purpose of its use, the role of the individual accessing the information, and so forth. These policies can be complex and specific, or broad as needed for a given type of data. Structured, policy-aware provenance logs of all information access events in the system are used to hold users accountable for their actions in a system [6].

In this paper we will demonstrate implementing the IAF protocols in FluxMED, a customisable EHR system designed to easily collect and manage different types of medical data [7]. FluxMED enables medical specialists to customise the handling of different types of data in a specialised way without changes to its code. Data collected in the system is highly structured, and use of the system is defined in workflows. Each activity in the system is made up of events such as a consultation, an exam or test performed, with specific information included in attributes.

Figure 1 illustrates how FluxMED can be used. Each step in the doctor's consultation or exams that have been requested or any other relevant information is represented by an activity in a workflow. FluxMED presents the set of activities that have been executed, and the set of new activities that can be executed at any point. In Figure 1, two activities have been executed, Identification, and First Index Event. There are three new activities that can be executed at this point, shown below in the second activity. In this case the user has selected the first of the new activities, and the right side frame shows the data that can be entered to register this activity. This example is

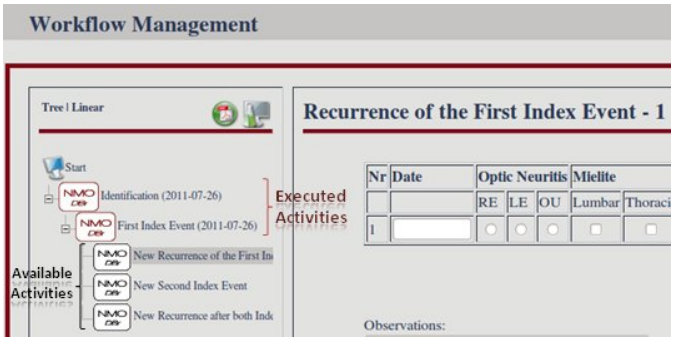


Fig. 1: FluxMED NMO-DBr Workflow

taken from the NMO-DBr, the Neuromyelitis Optica Database, developed with FluxMED [8]. FluxMED allows each activity to have a different set of access permissions, being an ideal platform to illustrate the functionalities of IAF protocols.

We begin our discussion in Section II with a description of the IAF protocols and how they can be applied. In Section III, we describe the FluxMED system. Section IV discusses how the protocols were implemented into the FluxMED workflows, and demonstrates their functionality within the system. Section V concludes the paper with a discussion of future work.

II. Information Accountability Framework

Information Accountability is a concept that involves using policies and mechanisms to enforce appropriate use through after-the-fact accountability for intentional misuse. IA mechanisms do not replace, but instead augment, traditional preventative measures that expect a user to be authorised to take an action in a system before attempting to do so. We define eHealth systems that implement IA mechanisms as Accountable-eHealth (AeH) systems.

By implementing non-restrictive access to information for legitimate users, AeH systems fulfil the information requirements of healthcare professionals. The presence of these IA mechanisms act as a deterrent for misuse to users through disincentives in the form of accountability entailed by penalties [9]. Misuse refers to the unauthorised access, use, modification, or disclosure of information, or other use of information that is not for the purpose for which the information was provided [10, 11]. Much like in the offline world we live in, it is expected that when users are aware of the accountability measures, they would not engage in inappropriate activities [12]. As a result, AeH systems allow information to be made available to legitimate users more openly and effectively without threatening patients' information privacy. The knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives for the subjects of the information, i.e. patients, to increase their trust in the system.

A primary concern that accountability protocols, such as those defined in the IAF, aim to address is with 'insider threats', which include accidental disclosures, insider curiosity and data breach by an insider [13]. Insider threats are a

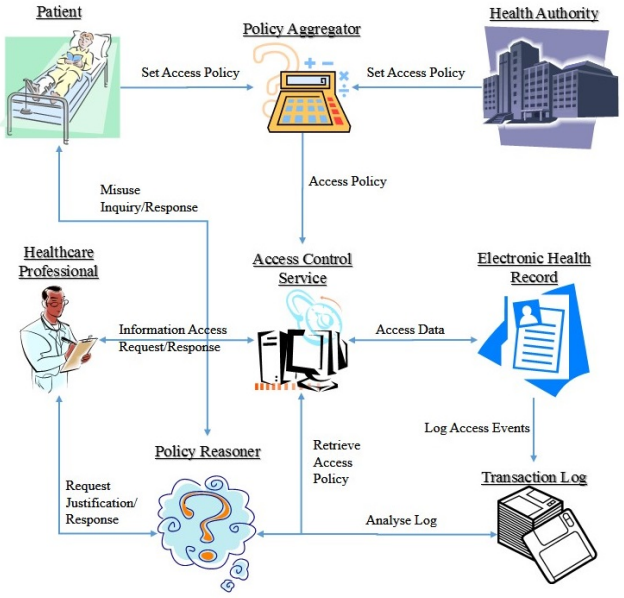


Fig. 2: Accountable-eHealth flow

significant issue when ensuring the privacy and security of patient data, with 17.5 percent of all health provider privacy breaches that were made public in the US between 2005 and 2014 being due to insider threats [14].

In devising the IAF for use in eHealth, we initially modelled four types of users: data owners (i.e patients), data users (i.e healthcare professionals) using health information for legitimate purposes, data users who misuse health information, and a central health authority (HA) (i.e. a government agency). Data owners have explicit control over which of their preferred HCPs can access their information and are able to set usage policies to grant or limit access further. The HA is in place to ensure that HCPs always have access to the information they need to provide appropriate care through setting default policies, without unnecessarily hindering the patient's privacy [15]. The patient and HA policies are amalgamated to produce a resulting usage policy for a given HCP.

As policy-aware transaction logs are a key component of accountability systems [16], in the IAF all information access and other events in the system are logged along with policy used to determine whether the action should be permitted. These logs provide the provenance of the information data in the system, which can be compared to usage policies to determine if an action complied with those policies [17]. The information these logs contain can also be considered sensitive and must be protected [18]. These logs are made available to the data owner in a user-friendly format which they can review at any time. The IAF actively monitors all actions taken in the system for potential breaches of policy and provides notifications as needed. For example, when a HCP makes an invalid access request, the system notifies the patient of the potential misuse of their eHealth information with a log that can be reviewed and referred to when submitting an inquiry

asking the HCP to justify their actions [6].

When the system detects possible misuse of a patient's health data, the patient is able to submit an inquiry asking for a justification of the actions taken by the relevant HCP. The HCP must then provide an explanation to justify their need to access the relevant information. Once this is done, the system uses a semantic reasoner and rules defined by a HA along with the context of the information access, usage policies, and the HCP's justification to determine whether misuse occurred and further investigation is required. An example of a possible flow of this model is shown in Figure 2.

This model has been validated using prototypes and surveys conducted into user acceptance, but it hasn't been fully implemented. In order to take a further step in the implementation of the IAF in eHealth systems and the development of AeH systems, we will demonstrate the use of the IAF in combination with the FluxMED EHR system.

When implementing the IAF protocols into an EHR system such as FluxMED either natively or as a service, it is important that the eHealth data is structured so that the type of data being accessed can be matched with usage policies. Additionally, the EHR system must be modified to log all events with the context of the event and policy used to permit or restrict access to the information. It must also be possible for HCPs to override patient usage policies when the need arises while the system provides clear communication to the HCP that their action is being recorded and may be investigated if misuse is suspected. This will often require appropriate changes to the front-end of the EHR system as we will demonstrate in FluxMED.

III. FluxMED

FluxMED is an EHR system that has been designed to be powerful and flexible. Typically EHR systems belong to one of two categories. They can be too rigid in the types of data that can be stored, limiting severely the symptoms, exams, diagnostics that can be used, allowing data only from the limited set of pre-specified information that has been coded into the system. Frequently doctors complain that such systems force them to enter the data in ways that are not appropriate because there is no way of changing the types of data that are accepted.

As a way of compensating for this problem, the other type of system is too generic, allowing the doctor to enter free text describing the patients consultation. Data entered in this way is very difficult to analyze, because each doctor specifies a different set of symptoms, treatments and so on. Frequently data from one consultation to the other is not comparable [19, 20].

FluxMED takes a different approach, making it possible to standardize the types of data entered by defining them in a workflow. These can be changed easily, incorporating new knowledge without changes to the system. It can be used in very flexible ways, for example, if different doctors follow different diagnostic strategies, that is, ask different questions, and request different exams, the workflow can incorporate both methods, and let the doctor choose which one to use.

Data entered in this way is structured to make it easy to analyze it later. Data is not entered in free text format, but in formats that have fixed types and requirements, which simplifies posterior analysis.

We have used FluxMED to develop EHR systems for three different diseases that are complex, difficult to diagnose and to treat. But because they are not common diseases, EHR systems aimed at them are non existant or very difficult to access. FluxMED has been able to model data from patients of neuromyelitis optica, paracoccidioidomycosis and adrenoleukodistrofy and enable doctors to use the system to initiate and follow patient treatments.

An important aspect of the FluxMED system is that creating a workflow for a new disease takes only a few hours with the help of a specialist. There is no need to change the system in any way. Moreover, new systems can be integrated with existing ones, so one EHR system can serve several specialities, making it simpler to maintain the data, train users and extend the system.

IV. Implementing the protocols into FluxMED

In FluxMED an EHR system is developed describing the steps in the doctors' consultation and treatment, and their attributes. For example, in Figure 1 we show a screenshot of NMO-DBr, the Brazilian Neuromyelitis database. In this case the doctor examines his patients by first identifying them through their name, address, and other information. This data is stored in the first activity of NMO-DBr. Once a patient is identified, the doctor can store what is called the First Index Event. This disease is rare and difficult to diagnose. Doctors establish their diagnostic by identifying what type of problems patients have, and if a certain number of crises occur the diagnostic is completed. Each crisis is called an Index Event. Several index events can occur, and NMO-DBr can store all of them and maintain their temporal relationship.

An EHR system inside FluxMED is then a series of activities, each recording an aspect of the patients symptoms and treatment. Symptoms and consultations can be stored as separate activities in FluxMED, as well as exams and treatments. The doctors using FluxMED then see the sequence of activities that have been registered, and can view each of them by selecting the activity name as seen in the left frame of Figure 1.

FluxMED has a powerful access control system that grants access permissions on an activity basis. In other words, permissions can be granted or not per activity. An example of usage could be for example, if you have four activities: 1. Identification; 2. Electrocardiogram exam; 3. Blood exam; 4. Diagnostic. Activities 2, 3 and 4 can only be executed after activity 1. Figure 3 shows how FluxMED sees this example.

The way IA is implemented in FluxMED is by assigning access permissions to each activity according to who can access them. One use would be that activities 1 and 4 can only be executed and by a general clinician. As shown in Figure 4,

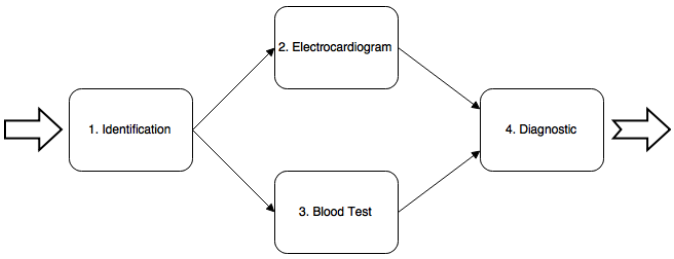
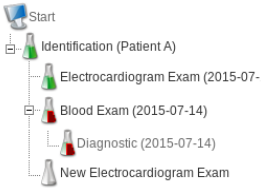
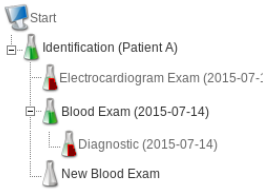


Fig. 3: A simple workflow illustrating IA in FluxMED

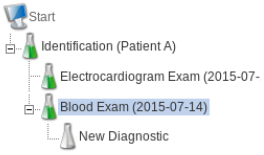


(a) Screen showing access as a cardiologist

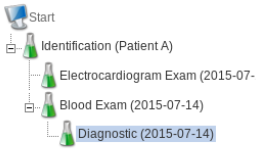


(b) Screen showing access as laboratory technician

Fig. 4: Screen behaviour under different roles



(a) Screen showing access as the general clinician



(b) Screen showing access as the data owner, or the Patient A

Fig. 5: Screen behaviour under different roles

User	Date and time	Data	Potential Misuse?	Reason
General Clinican	2015-07-14 17:51:47	Blood Test	No	-
Cardiologist	2015-07-14 18:30:23	Electrocardiogram Exam	No	-
Lab Technician	2015-07-14 19:07:45	Blood Test	No	-
Endocrinologist	2015-07-14 21:34:05	Blood Test	Yes	Possible diabetes

Fig. 6: Possible information misuse are highlighted in FluxMED

cardiologists can view activity 1 and execute activity 2, lab technicians can view activity 1 and execute activity 3, and the general clinician can view all activities. In this way, the general clinician can view all exams and make the diagnostic. Cardiologists and lab technicians can view the identification so they will know who to exam. They will register their exams, but will not see exams performed by other personnel.

Finally, the complete set of activities, called an instance in FluxMED has as owner the patient who can see all four activities and change permissions for his or her data.

One additional aspect of the IA protocols is, naturally accountability. FluxMED registers all access activity in the system. Each execution or modification of an activity is registered. In addition to that, activities visualization is also registered. So, if a user chooses to visualize an activity, this fact is also registered in the system, so the patient can see a full history of doctors and others healthcare professionals that accessed his data, if they actually had enough privileges to see this information (Figure 6).

This is a key point of the implemented protocol: the access must be non-restrictive. A doctor, as a healthcare professional, must have the access granted to any data of their patients if he considers it necessary, for example, in an emergency case. On the other hand the healthcare professional can be investigated by the healthcare authority if the information is misused.

V. Conclusion and Future Work

The use of information accountability protocols enables the creation of eHealth records that can be useful to both consumers and healthcare professionals. By ensuring transparency and accountability is applied, data owners (i.e. patients) are aware of how and why their information is accessed and used, while medical professionals are able to access all the information they need to provide care to their patients and make informed decisions. As a result, accountable-eHealth systems create an environment where health information is available to the right person at the right time without rigid barriers, whilst empowering the consumers with control over the use of their information.

In this paper, we have taken one step closer to realising accountable-eHealth systems through implementing them in a full EHR system, FluxMED, and demonstrating the functionality of the IAF protocols. Using this implementation, we are working to further validate the approach through user testing with the healthcare professionals and other users of FluxMED.

References

[1] T. Sahama, L. Simpson, and B. Lane, "Security and privacy in ehealth : is it possible? a sociotechnical analysis," in *15th International Conference on e-Health Networking, Applications and Services*, J. R. Rodrigues, Ed. Lisbon, Portugal: IEEE, August 2013, to be published in the IEEE Healthcom 2013 Conference Proceedings and IEEEXplore.

[2] J. Boyd, *Accountability*. McMurry Inc., 2003, vol. 69.

[3] W. M. Tierney, S. A. Alpert, A. Byrket, K. Caine, J. C. Leventhal, E. M. Meslin, and P. H. Schwartz, "Provider responses to patients controlling access to their electronic health records: A prospective cohort study in primary care," *Journal of General Internal Medicine*, vol. 30, no. 1, pp. 31–37, 2015. [Online]. Available: http://dx.doi.org/10.1007/s11606-014-3053-0

[4] Department of Health, "Personally Controlled Electronic Health Record Review Report," 2014. [Online]. Available: http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth

[5] R. Gajanayake, R. Iannella, and T. R. Sahama, "Sharing with care: An information accountability perspective," *IEEE Internet Computing*, vol. 15, no. 4, pp. 31–38, August 2011.

[6] D. Grunwell, R. Gajanayake, and T. Sahama, "Demonstrating accountable-ehealth systems," in *Proceedings of IEEE International Conference on Communications 2014*, IEEE. IEEE, June 2014, pp. 4258–4263.

[7] A. C. Faria-Campos, L. Hanke, P. H. Batista, V. Garcia, and S. Campos, "Fluxmed: An adaptable and extensible electronic health record system," in *Advances in Bioinformatics and Computational Biology*, ser. Lecture Notes in Computer Science, S. Campos, Ed. Springer, 2014, vol. 8826, pp. 33–40.

[8] M. A. Lana-Peixoto, L. E. Talim, A. C. Faria-Campos, S. V. Campos, C. F. Rocha, L. A. Hanke, N. Talim, P. H. Batista, C. R. Araujo, and R. Kleinpaul, "Nmo-dbr: the brazilian neuromyelitis optica database system," *Arquivos de neuro-psiquiatria*, vol. 69, no. 4, pp. 687–692, 2011.

[9] J. Feigenbaum, A. D. Jaggard, and R. N. Wright, "Towards a formal model of accountability," in *Proceedings of the 2011 workshop on New security paradigms workshop*. ACM, 2011, pp. 45–56.

[10] Privacy Act 1988, Clth. [Online]. Available: http://www.comlaw.gov.au/Details/C2013C00231

[11] Health Identifiers Act 2010, Clth. [Online]. Available: http://www.comlaw.gov.au/Details/C2010C00440

[12] J. Feigenbaum, J. Hendler, A. D. Jaggard, D. J. Weitzner, and R. N. Wright, "Accountability and deterrence in online life," in *Proceedings of the 3rd International Conference on Web Science*. ACM, 2011.

[13] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279–314, 2010.

[14] Privacy Rights Clearinghouse, "Chronology of Data Breaches," n.d., Accessed January 2015. [Online]. Available: https://www.privacyrights.org/data-breach

[15] D. Grunwell, R. Gajanayake, and T. Sahama, "Improving usefulness of ehealth systems through information accountability," *e-Health Technical Committee Newsletter*, vol. 2, no. 6, pp. 3–5, December 2013.

[16] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," *Communications of the ACM*, vol. 51, no. 6, pp. 82–87, 2008. [Online]. Available: http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf

[17] R. Aldeco-Pérez and L. Moreau, "Provenance-based auditing of private data use," in *International Academic Research Conference, Visions of Computer Science*. BCS, September 2008.

[18] D. Grunwell, R. Gajanayake, and T. Sahama, "The security and privacy of usage policies and provenance logs in an information accountability framework," in *Eighth Australasian Workshop on Health Informatics and Knowledge Management*, A. Maeder and J. Warren, Eds. Sydney, Australia: Australian Computer Society, 2015, pp. 33–40.

[19] S. Asabe, N. Oye, and M. Goji, "Hospital patient database management system: A case study of general hospital north-bank makurdi-nigeria," *Compusoft*, vol. 2, no. 3, pp. 65–72, March 2013.

[20] K. S. Sim, S. S. Chong, C. P. Tso, M. E. Nia, A. K. Chong, and S. F. Abbas, "Computerized database management system for breast cancer patients," *SpringerPlus*, vol. 3, no. 268, pp. 1–16, 2014.