5-2012

Information Accountability with Policy Languages for e-Health

Randike Gajanayake
Queensland University of Technology, g.gajanayake@qut.edu.au

Renato Iannella
National E-Health Transition Authority, renato.iannella@nehta.gov.au

Tony Sahama
Queensland University of Technology, t.sahama@qut.edu.au

Information Accountability with Policy Languages for e-Health

Randike Gajanayake
Queensland University of Technology
g.gajanayake@qut.edu.au

Renato Iannella
National E-Health Transition Authority
renato.iannella@nehta.gov.au

Tony Sahama
Queensland University of Technology
t.sahama@qut.edu.au

Abstract
ICT is becoming a prominent part of healthcare delivery but brings with it information privacy concerns for patients and competing concerns by caregivers. A proper balance between these must be established in order to fully utilise ICT capabilities in healthcare. Information accountability is a fairly new concept to computer science which focuses on fair use of information. In this paper we investigate the different issues that need to be addressed when applying information accountability principles to manage healthcare information. We briefly introduce an information accountability framework for handling electronic health records (eHR). We focus more on digital rights management by considering data in eHRs as digital assets and how we can represent privacy policies and data usage policies as these are key factors in accountability systems.

Keywords
Healthcare, eHR, ICT, e-health, privacy, fair use, information accountability, transparency, provenance, policy, DRM, ODRL.

1. Introduction
Information and Communication Technology (ICT) is becoming a prominent part of healthcare delivery. But issues such as information security and privacy concerns have hindered its progression towards improving healthcare delivery. The use of ICT in healthcare has given rise to a comparatively new informatics domain called e-health. Electronic health records (eHR) are the driving force behind e-health. An eHR is a complete record of a patient's medical history which may include information pertaining to sensitive concerns such as sexual health, mental health, addictions to drug or alcohol, abortions etc. Due to this reason patients demand strong security for their eHRs. Without trusting that their sensitive health information will be safeguarded, patients are reticent to fully and honestly disclose their personal information and may avoid seeking care altogether (Goldman and Hudson 2000).

Unlawful disclosure of personal information could cause the subject of the information embarrassment and may affect insurability, child custody cases, and even employment (Pratt, Unruh et al. 2006; Cannoy and Salam 2010). Therefore, informational privacy is vital to ensure the reliability of eHR systems. Alan Westin, in his book "*Privacy and Freedom*", defines privacy as "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin 1967), i.e. control of private information. Others argue that data confidentiality addresses privacy requirements. Confidentiality means giving the information *owner* the control of the information whereas privacy deals with giving the *subject* of the information control over it. Data ownership is itself subject to disparity in different contexts. However, a significant degree of control over personal information is essential to protecting information privacy (Solove 2008).

Access to sensitive information must be handled with rigor and vigilance. Various methods have been proposed to address the privacy conundrum ranging from strict access control to privacy-preserving algorithms such as anonymization (Bayardo and Agrawal 2005), generalization (Sweeney 2002), and perturbation (Kargupta, Datta et al. 2003). However, these techniques may discourage honest and legitimate users from accessing data required to fulfill genuine tasks. Access control mechanisms either permit or deny access, there are no intermediate states. They are not policy-aware and may also hinder the actions of legitimate users of an information system (Kagal and Pato 2010). According to Kagal et al. (2010) access control mechanisms alone are inadequate for privacy protection.

Information accountability (IA) complements access control mechanisms and supports policy-awareness. In theory, the principles behind IA would make sure that the information users follow the appropriate rules and policies. To facilitate IA principles, systems should implement usage policies on its assets. Data in eHRs can be considered as digital assets. Data management in e-health thus entails digital rights management (DRM). Privacy policies in e-health can be represented using an appropriate digital rights expression language (REL). Policies on the use of data in an eHR can be set by the patient, a trusted healthcare representative, a health authority or all the above.

The contribution of this paper is an information accountability framework (IAF) for eHR systems and the structure of the policy representation in the framework. The IAF is built on IA principles which we will discuss in section 3. We will illustrate data usage policy representations for eHRs using the open digital rights language (ODRL) with the aid of a simple case scenario.

2. Information Accountability

A serious concern for accountability systems is the lack of formal foundations. Formalising information accountability has been widely explored by many in recent work (Lampson 2005; Weitzner, Abelson et al. 2008; Jagadeesan, Jeffrey et al. 2009; Sloan and Warner 2010; Feigenbaum, Hendler et al. 2011; Feigenbaum, Jaggard et al. 2011). Feigenbaum et al. (2011) claim that a purely preventive approach to security is inadequate, thus supporting the claim by Kagal et al. (2010). They investigate some existing frameworks for accountability and explore whether deterrence is a better term than accountability and puts forth a formal model for accountability in terms of punishment (Feigenbaum, Jaggard et al. 2011). Assuming that the

relevant privacy policies exist, Jagadeesan et al. (2009) make an effort to develop formal foundations for information accountability in terms of the privacy policies which define appropriate sharing of information among agents and provides algorithms that can be used by an auditor to check for compliance with rules.

A solution to the question of compliance of privacy policies is proposed by Weitzner et al. (2008) by tracking all transactions and making them transparent. They assume that appropriate policy rules exist with a formal representation, policy-aware transaction logs and a policy-reasoning capability which would enable accountability systems to hold information users (individuals and organisations) accountable for their actions. With a strong focus on the facts Weitzner et al. (2008) put forth, Sloan et al. (2010) address information accountability in broader scope by considering social policies and technical aspects. They point out that automated checking for compliance of privacy policy is a necessity for accountability systems and without the adequate foundations in both formal models and public policy issues they are unlikely to do so. They believe that policies required to developing accountability systems are informational norms and state that a proper balance between privacy requirements and competing concerns is necessary to sustain the architectural and social aspects introduced by Weitzner et al. (2008).

Defining a general formula for IA with the current ambiguous nature of the concept is a difficult feat and would not directly benefit the development of accountability systems which is the ultimate goal. We believe that contextual definitions would be more suitable in that the characteristics of the policies, if not the proper policies themselves, can be developed.

2.1. Principles of Information Accountability

In computer science, access control and accountability are closely related. Access control is about restrictions, whereas accountability is about punishment. Therefore, *audit logs* are an essential part of an accountability system (Lampson 2009). In any information system all trust is within the system, outsiders cannot be held accountable. We cannot hold everyone accountable, it is crucial that we identify who can be held accountable and who cannot. Therefore, an accountability system should have strong system *boundaries*. Accountability systems facilitate *fair use* of information. Rather than prevention via rigid locks on data, accountability is about *deterrence*. The presence of an accountability mechanism deliver a threat of punishment which would deter users from intentional misuse. Accountability systems should facilitate *transparency* such that all relevant parties have the capability to observe how information is used and by whom. This makes *bad acts visible* and helps deter users from misuse.

The users of an accountability system should be *well informed*, i.e. a notification process where users are informed about underlying policies before an action occurs must be put in place. For example a user will be notified whether he is authorised to access/use a particular set of data he is trying to access/use and the ramifications if he proceeds regardless of the warning. This will also help in facilitating non-repudiation which is a significant aspect in information security. All users of the system are kept informed of relevant transactions by the *Message Engine* and related services in the IAF below.

When holding someone accountable, trustworthiness of the data about the inappropriate transaction(s) is important. Hence, *provenance* of data and metadata is a significant factor in information accountability. As Moreau et al (2008) point out, electronic data does not have the

necessary historical information that would help end-users, reviewers or regulators make the necessary verifications. In an accountability system provenance can be facilitated using appropriate transaction logs (*Policy aware Transaction Logs* and *Transaction Metadata Engine* in Figure 1). These transaction logs also serve another purpose in terms of accountability by being *policy-aware*. Policy-aware transaction logs can also facilitate *policy reasoning* capabilities (facilitated by the *Policy Reasoning Engine* in Figure 1) and enable the users to reason about misuse and against claims of misuse.

Creating proper *incentives* that would make consumers follow rules of accountability systems is important (Sloan and Warner 2010). For an information user, the threat of punishment for misuse is an incentive to follow system rules. An incentive such as a strong assurance of privacy should be given to patients to prevent them from withholding information or enforcing rigid restrictions on data which would be their obvious cause of action to secure their information.

2.2. Information Accountability in Healthcare

In order to understand the concept of information accountability in healthcare, it is important to clearly identify the different parties in healthcare that can be held accountable, the issues for which a party can be held accountable and the appropriate mechanisms for accountability in healthcare (Emanuel and Emanuel 1996). The National E-Health Transition Authority (2011) has identified several types of roles with different capabilities in their new Personally Controlled Electronic Health Record (PCEHR) system; individuals, nominated representatives, authorised representatives, providers and nominated providers. Policies should be developed that address the different capabilities of roles within the industry. These policies should capture the requirements of all relevant parties. In a healthcare domain it is difficult to define who owns health information. It is clear that patients are the subjects of health information. But patients are not always medical professionals; hence it is impossible to give them full control of their health information. Privacy policies should accompany an input from a professional health body such as a trusted medical practitioner or a central health authority. But it is important to balance between the patient's privacy requirements and the requirements of the healthcare providers or the care givers (competing concerns).

In a healthcare setting, the patient's privacy policies cannot contradict those set by the healthcare providers or the health authority. The IMIA code of ethics for medical information professionals (International Medical Informatics Association 2002) states under their first ethics principle that "*All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves"*. Taking this to consideration let us devise the following general requirements of a patient with an eHR: 1) the capability to control access to the eHR by allowing only a preferred set of medical practitioners access to the eHR, 2) the capability to hide certain health information from health practitioners who already have access to their eHR, 3) the capability to check how the eHR is manipulated by authorised users, 4) the capability to inquire about concerning usage. Let us also consider a the following requirements of healthcare practitioners: 1) the capability to define their security policies within the organization, 2) access to the relevant information in a non-restrictive and timely manner, 3) the capability to share patient health information with other health specialists, 4) the capability to override patients' security settings in special circumstances (e.g. life threatening emergency

situations, mental health related situations). We take these requirements in to consideration when designing our IAF for eHR systems. It is important to note that usage policy enforcement might not always be beneficial to the patient. While fulfilling these privacy requirements under no circumstance must the health of the patient is compromised. A compromise between the requirements must entail the final policy representation of the systems and the proper integration of these policies would improve patient confidence in the system. Clear procedures for overriding usage policies in emergency situations should be defined. The nature of the healthcare domain forces the implementation of a *break the glass* approach in emergency situations.

Apart from the requirements stated above, certain circumstances might require some health conditions be kept hidden from the patients. For example this may be the case for patients suffering from severe mental health conditions where the knowledge of particular illnesses may aggravate existing health conditions. They may also be considered unfit to manage their eHRs. We acknowledge this eventuality but consider them as rare occurrences and do not integrate such capabilities in to the framework. However, in such cases the control over the patient's eHR may be given to a custodian or a trusted health professional (HP) such as the patients GP who can take the patient's role in controlling the eHR.

3. Information Accountability Framework for EHR Systems

Considering the information accountability principles and the contextual requirements of healthcare discussed above, we designed the information accountability framework (IAF) for e-health systems depicted in Figure 1. Due to space restrictions we shall only give a brief overview of the IAF in this paper.

The core components of the IAF are the privacy-aware policy engine, the policy-aware transaction logs and the policy reasoning engine within the policy engine. The IAF has inputs from the patients, the health authority and health professionals who wish to access/use information. The policy aggregator engine will amalgamate the patient's policies and the health authority's policies. This amalgamation is done in such a way that the patient's privacy requirements are met and the health authorities' policies be satisfied. HPs are required to lodge a *usage request* before they are able to access the eHR data. If their requests are satisfactory they are provided with the requested data. Necessary notifications are sent to patients about the activities on their eHR data. The patients are able to lodge *usage inquiry queries* on certain episodes of information usage. The health professionals can answer those queries by lodging *reasoning queries* as to why they have done so. All queries made by the actors are policy aware. Hence the need for *policy-aware* transaction logs.

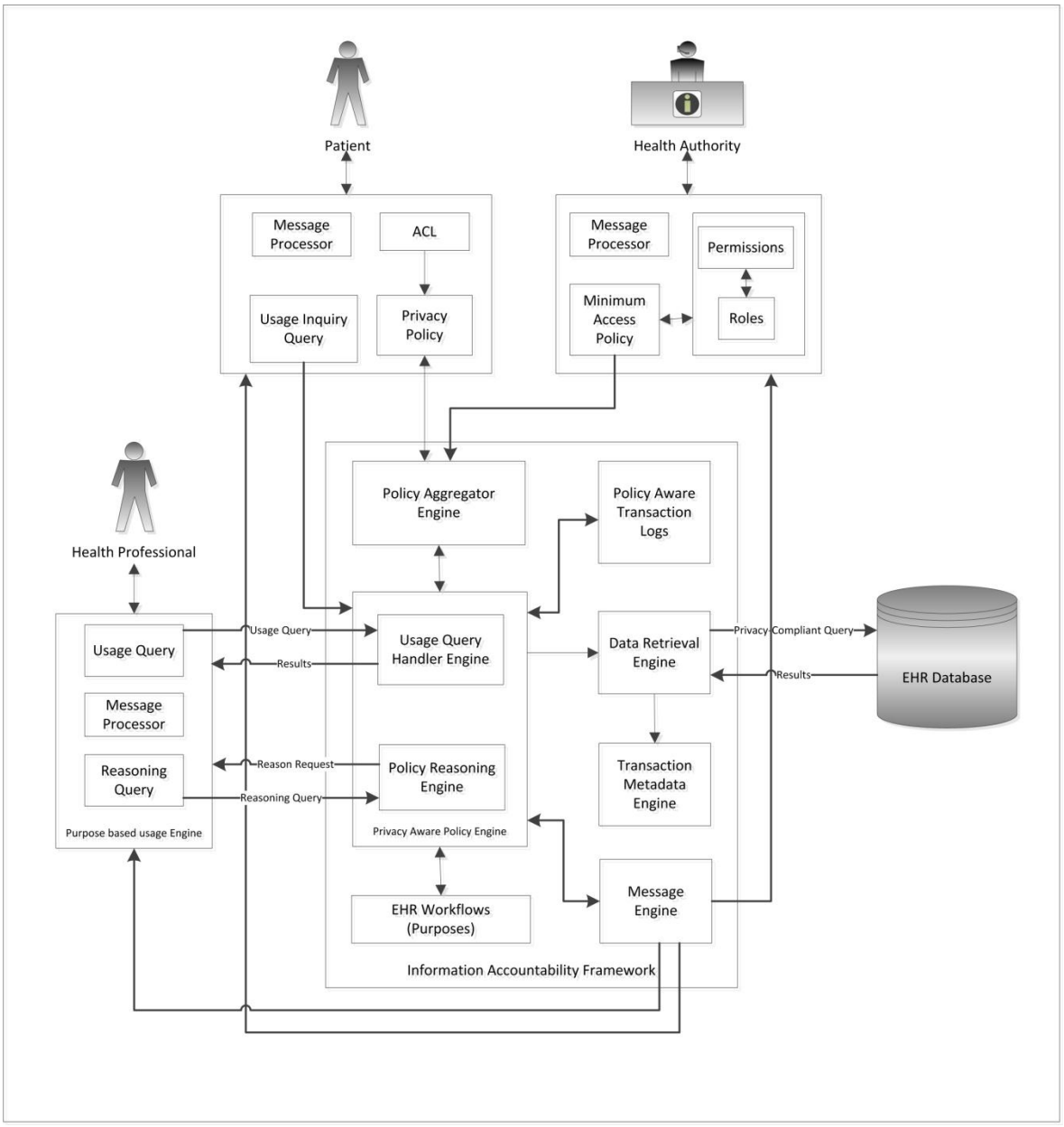

Figure 1: Information Accountability Framework for eHRs

We note here that NEHTA's PCEHR (National E-Health Transition Authority 2011) system describe an audit mechanism to improve consumer confidence in disclosing information in the system. It provides the consumers the capability to investigate the use of information by care providers. Their real time audit system differs from what we propose in that it is not explicitly policy or privacy aware. The policy and privacy aware audit mechanism in our IAF will enable the consumers to be more independent and would help towards giving the patients more control of their health information.

3.1. Digital Rights Management

The advancement of ICT, especially the role of the Internet, has led to the need of proper protection of digital media such as music-files, video-files, etc. Digital contracts were developed to control the flow and use of information. These contracts were expressed using digital property rights languages. Such technologies are known as digital rights management (DRM). DRM technologies are well known for their role in copyright protection of media files on the Internet and are becoming a prominent resource in protecting private information of individuals (Feigenbaum, Freedman et al. 2002). DRM has many similarities to the traditional access control model but differs in that they require information to remain protected even after access is granted. DRM deals with usage control of information resources by authorised users. Each piece of information is protected by a usage license created by the digital rights holder. DRM can benefit e-health technologies by providing a means to manage the use and control of patient electronic health records. The patients and the health authority have the rights to manage the usage licenses which can be expressed in Rights Expression Languages (REL). RELs are a critical aspect of DRM systems. RELs such as XrML (ContentGuard 2011) and the Open Digital Rights Language (ODRL Initiative 2012) are prominent among others.

The ODRL rights expression language provides a syntax and semantics to express policies related to digital assets. The ODRL core model is formally specified using UML notation and aims to be independent from implementation constraints and is able to express a wide range of policy-based information (ODRL Initiative 2012). In the next sections we will show how patient privacy policies and other eHR requirements can be represented in ODRL expressions.

3.2. Healthcare Scenario

Consider the following scenario. Gary has a comprehensive eHR. This eHR is formulated such that each type of data (e.g. identity data, general health data, dental health data, mental health data, etc.) can be distinguished by eHR data type identifiers. For each of these data types there exists a set of predefined purposes for which those data can be used. The purposes are defined by a central health authority considering all necessary requirements to address every episode of care. Gary has a list of trusted healthcare providers (health professionals) to whom he may give access to data in his eHR. Peter is Gary's GP, Sandra is a dermatologist, Bill is a sexual health specialist and Matt is a mental health specialist who has treated Gary in the recent past. Gary can set privacy settings to govern the access to his eHR. A central health authority can also set access settings to patient's eHR by considering the roles of each health professional.

3.2.1. Scenario

After noticing a skin rash, Gary visits his trusted dermatologist Sandra for a check up. After a preliminary examination, Sandra thinks that Gary's skin condition could be linked to a known sexually transmitted disease (STD). Gary does not have a sexual health specialist in his list of trusted health professionals. However, Sandra wants to share Gary's details with a sexual health specialist, Bill, in order to get a specialists opinion on the situation. Bill has a default access level set by the health authority to be able to access patients' sexual health details and dermatology details. Since Sandra is in Gary's list of trusted HPs to be able to access Gary's dermatology information, she can initiate a request to share Gary's details with other health professionals. Gary, however, is notified of this action by Sandra. After Bill gets this request, he initiates a usage request to use the data for diagnosis purposes. Gary has a history of mental

illness and does not want anyone else other than his GP (Peter) and a trusted mental health specialist who treated him (Matt) to know about it. At some point during or after this episode of care, Gary may include Bill to his list of trusted health professional.

3.2.2. Scenario with ODRL

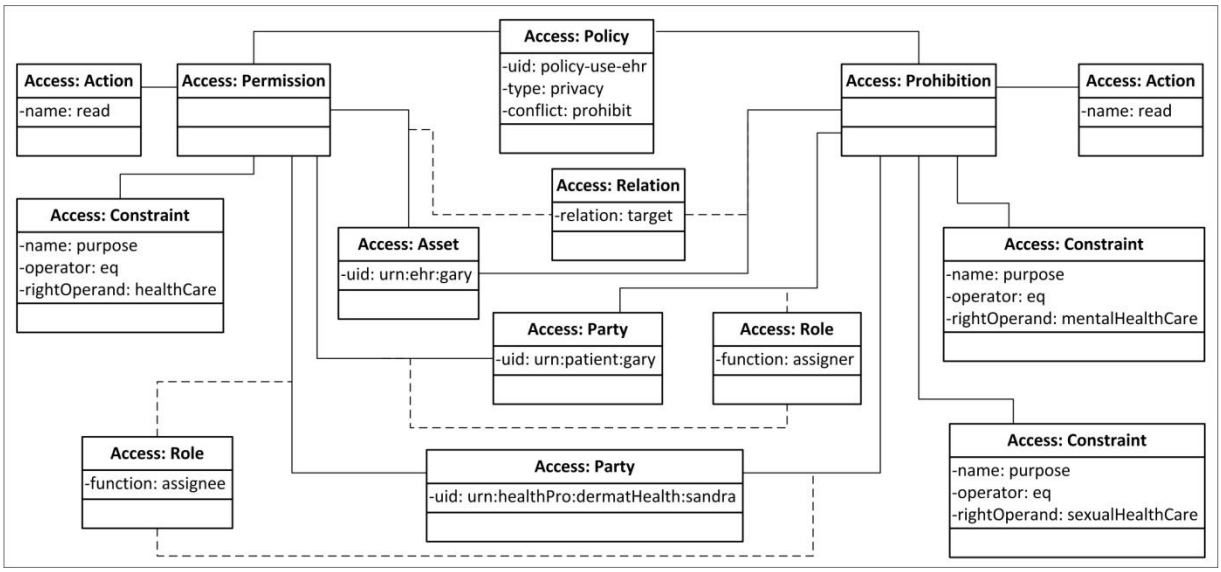

Figure 2: Settings for Sandra by Gary

The ODRL XML Encoding for the UML in Figure 2 is as follows.

```
<o:policy xmlns:o= "http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="http://w3.org/ns/odrl/2/privacy"
uid="policy-use-ehr" conflict="o:prohibit">
        <o:permission>
                <o:asset uid="urn:ehr:gary" relation="o:target"/>
                <o:party uid="urn:patient:gary" role="o:assigner"/>
                <o:party uid="urn:healthPro:dermatHealth:sandra" role="o:assignee"/>
                <o:action name="o:read"/>
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:healthCare"/>
        </o:permission>
        <o:prohibition>
                <o:asset uid="urn:ehr:gary" relation="o:target"/>
                <o:party uid="urn:patient:gary" role="o:assigner"/>
                <o:party uid="urn:healthPro:dermatHealth:sandra" role="o:assignee"/>
                <o:action name="o:read"/>
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:sexualHealthCare"/>
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:mentalHealthCare"/>
        </o:prohibition>
</o:policy>
```

In the privacy policy above, Gary gives Sandra permission to access his entire health record and prohibits her from accessing his sexual health and mental health details. The conflict attribute of the policy is set to "*prohibit*" indicating that prohibitions take precedence in the

policy. Gary's settings for other trusted HPs have the same structure while attribute values change accordingly.

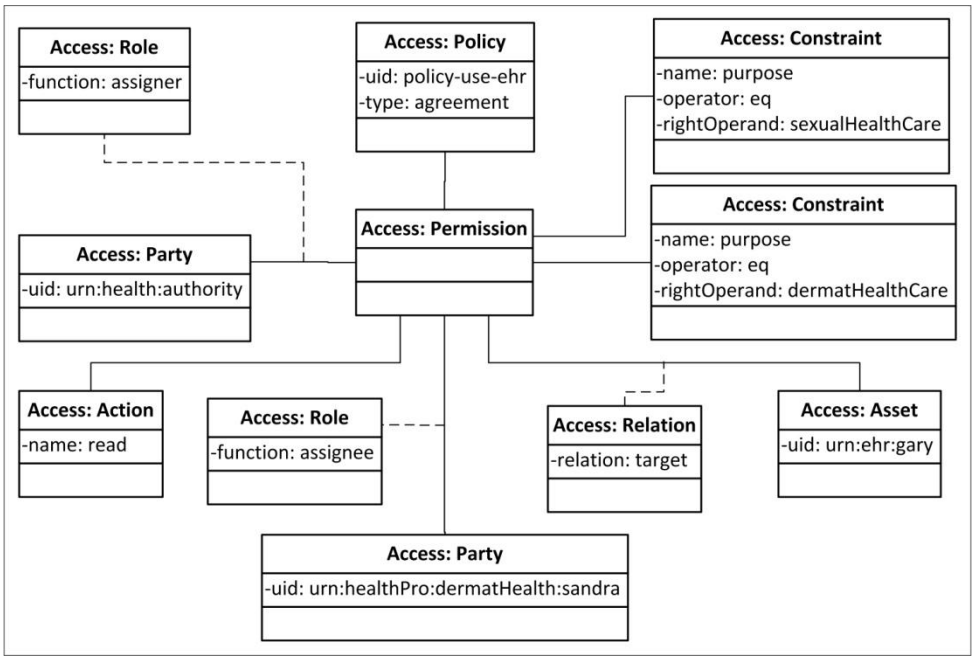

Figure 3: Settings for Sandra by the health authority

The ODRL XML Encoding for the UML in Figure 3 is as follows.

```
<o:policy xmlns:o= "http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/agreement" uid="policy-use-ehr">
        <o:permission>
                <o:asset uid="urn:ehr:gary" relation="o:target"/>
                <o:party uid="urn:health:authority" role="o:assigner"/>
                <o:party uid="urn:healthPro:dermatHealth:sandra" role="o:assignee"/>
                <o:action name="o:read"/>
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:dermatHealthCare">
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:sexualHealthCare">
        </o:permission>
</o:policy>
```

The health authority is responsible for setting default access policies for specific healthcare roles, in this case for the role of a dermatologist. In the policy in Figure 3 the health authority gives Sandra the permission to access Gary's dermatology details and sexual health details. Note here that Gary's settings prohibit Sandra from accessing his sexual health details. But we assume a hypothetical scenario where a relationship between skin conditions and STDs exist, and every dermatologist should have access to the patient's sexual health details. The health authority is aware of this fact and allows all dermatologists access to patients sexual health details. The settings by the health authority always prevail over patient settings. The patient however will be given notice of this before any actions occur on the data. Similar relationships

may be present in the medical field. Therefore, an input from an entity with the relevant medical knowledge is essential in the formulation of policies of this nature. The final policy will be a combination of the two policies and hence the requirement for a policy aggregation engine in our IAF. The patient is given due notice of this before any actions occur on the data. Any usage requests by Sandra are compared with this aggregated policy and if compatible, the requested usage licenses are issued. In the case of an incompatible usage request, the user is given notice as to why the license is not issued and the user can choose to comply with the existing policy or to override it. In such a situation the patient is notified about possible misuse of information.

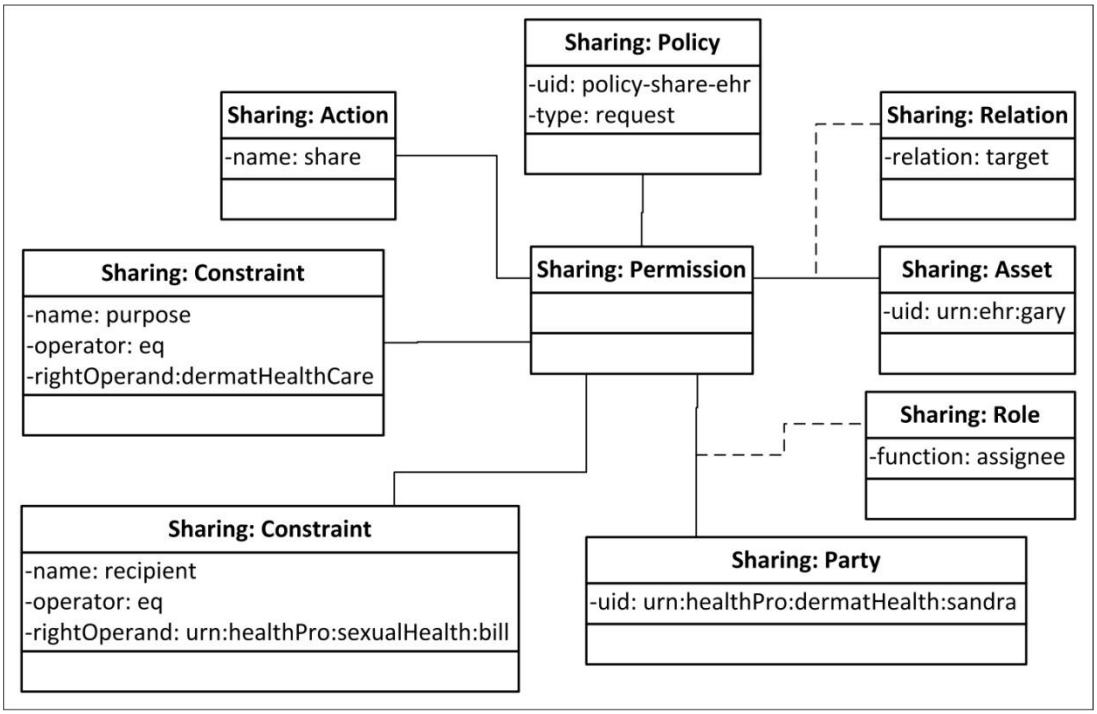

Figure 4: Request to share Gary's data with Bill

The ODRL XML Encoding for the UML in Figure 4 is as follows.

```
<o:policy xmlns:o="http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="http://w3.org/ns/odrl/2/request"
uid="policy-share-ehr">
        <o:permission>
        <o:asset uid="urn:ehr:gary" relation="o:target"/>
        <o:party uid="urn:healthPro:dermatHealth:sandra" role="o:assignee"/>
        <o:action name="o:share"/>
        <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:dermatHealthCare">
        <o:constraint name="o:recipient" operator="o:eq" rightOperand="urn:healthPro:dermatHealth:bill">
        </o:permission>
</o:policy>
```

The policy in Figure 4 represents Sandra's request to the eHR system to share Gary's dermatology details with Bill. If Sandra is granted with the license for this policy she can

initiate the sharing process. After the initiation, Bill will have access to the eHR Data stated in the policy but still has to request a usage license from the eHR system. This is given in Figure 5. In this policy Bill requests a license to *read* Gary's dermatology details for the purpose of a dermatology related episode of care (*dermatHealthCare*).

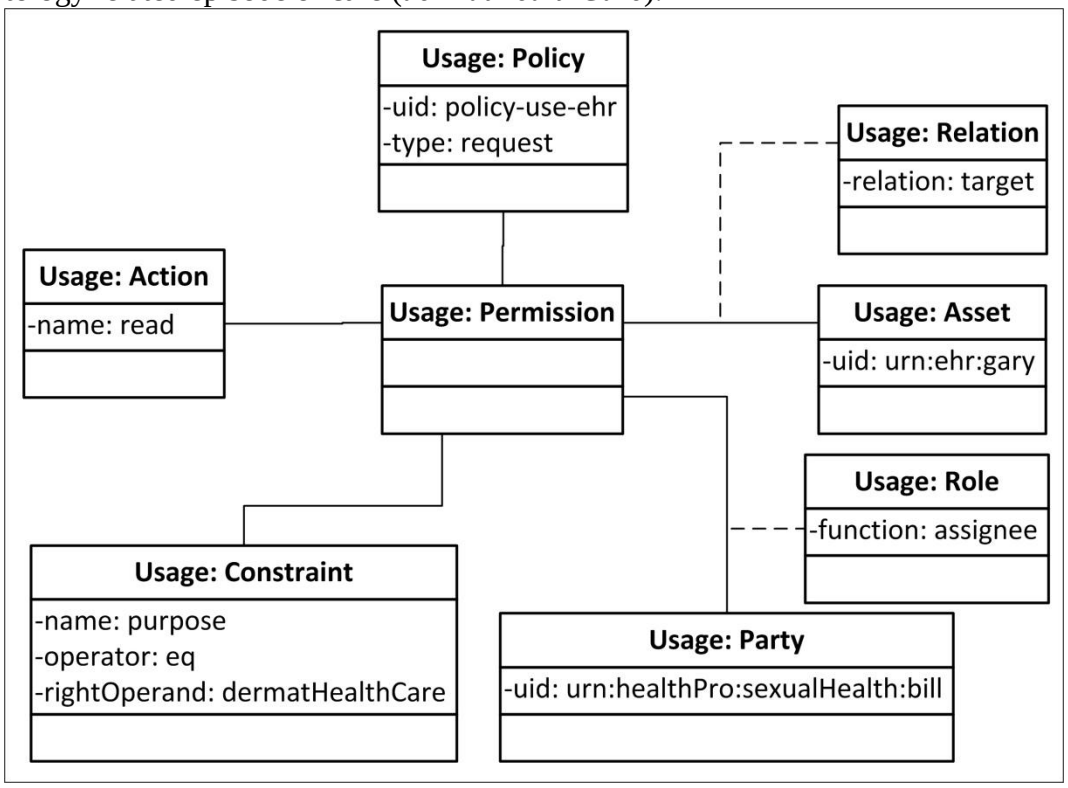

Figure 5: Usage request by Bill

The ODRL XML Encoding for the UML in Figure 5 is as follows.

```
<o:policy xmlns:o= "http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type=" http://w3.org/ns/odrl/2/request"
uid="policy-use-ehr">
        <o:permission>
                <o:asset uid="urn:ehr:gary" relation="o:target"/>
                <o:party uid="urn:healthPro:sexualHealth:bill" role="o:assignee"/>
                <o:action name="o:read"/>
                <o:constraint name="o:purpose" operator="o:eq" rightOperand="eh:dermatHealthCare">
        </o:permission>
</o:policy>
```

Usage requests by users are compared with the predefined policies and if satisfied, the licenses are issued. In this case however, Bill's usage request will be compared with the sharing request initiated by Sandra since Bill is not currently in the trusted list of health professionals. Using this policy representation we can clearly define patient privacy concerns and the requirements of the healthcare domain in terms of information access. Individual HPs can also implement their access requirements with the consent of the patients. With this representation

we fulfill the first requirement for accountability systems. Policy-aware transaction logs, policy reasoning and the other components of the IAF can be developed over the existing policy platform.

4. Discussion

In this paper we have investigated information accountability and its application in healthcare. We identified several key aspects of IA via related literature. We presented an IAF for eHRs that would enable us to develop an accountability system for e-health. It is clear that IA is a new concept to computer science and the proper definition of its principles is still in its infancy. This is a significant barrier for systems developers to build systems that are IA compliant. We believe that it is suitable to define or rather formulate the foundations for accountability systems contextually. This would enable the system developers to gain a clearer insight of the requirements of the system.

Privacy policy representation is a significant part of accountability systems. The arrangement of policies varies depending on the nature of the information being protected and the nature of the industry. For example, it is unclear as to who the actual owners of health information are. This led us to introduce a policy aggregator engine to our IAF to amalgamate privacy policies of the patients and the policies of a health authority. In a realistic scenario patients would be given control of their eHR at a suitable age put forward by a relevant authority.

Being policy driven, the proper representation of the necessary policies is essential in accountability systems. As a first step towards implementing the proposed IAF, we used the open digital rights language for representing the various policies in the system. ODRL v2.0 is a work in progress release which gave us the flexibility to accommodate certain requirements of the healthcare domain. In order to implement the IAF a comprehensive set of attribute values need to be defined. We have presented a simple scenario to demonstrate the policy representations. Due to space restrictions we are unable to present a complete set of policy representations in this paper.

A policy reasoning capability should be facilitated by an accountability system. This allows the users (e.g. patients) to investigate possible breaches of policy and the accused (e.g. health professionals) to defend their actions. But not all actions should be subject to such investigation which would disrupt activities of care givers. The system being policy-aware would identify possible breaches of policy and inform the relevant party giving them the opportunity to take action.

5. Conclusion and Future Work

Accountability systems aim at keeping information safe from unnecessary disclosure and misuse by making bad acts visible to all concerned and deter users from misusing information by holding them accountable for misuse. Making this a reality is no easy feat. It involves the collaboration of experts from several disciplines including social science, law, computer science, and specialists form the domain for which the system is developed. The IAF presented in this paper follows IA principles in the healthcare context. We have explored a means of representing privacy policies in a machine readable manner which we intend to extend for policy reasoning, policy-aware audit logs and ultimately for determining policy compliance of

information users. There is considerable amount of work to be done to make the IAF a comprehensive tool for the implementation of accountability systems. We are currently working on the implementation of this IAF to demonstrate its functionality in a simulated healthcare environment. We are working to extend the ODRL model to support policy reasoning to fulfill the requirements for accountability systems.

6. Acknowledgements

We would like to thank the National Information and Communications Technology Australia (NICTA) for partially funding this ongoing research project.

References

Bayardo, R. J. and R. Agrawal (2005). Data privacy through optimal k-anonymization. Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on.

Cannoy, S. D. and A. F. Salam (2010). "A framework for health care information assurance policy and compliance." Commun. ACM **53**(3): 126-131.

ContentGuard. (2011). "Extensible Rights Markup Language." Retrieved 18/11/2011, from http://www.xrml.org/.

Emanuel, E. J. and L. L. Emanuel (1996). "What Is Accountability in Health Care?" Annals of Internal Medicine **124**(2): 229-239.

Feigenbaum, J., M. J. Freedman, et al. (2002). "Privacy Engineering for Digital Rights Management Systems." Lecture Notes in Computer Science, Security and Privacy in Digital Rights Management **2320**: 76-105

Feigenbaum, J., J. Hendler, et al. (2011). Accountability and Deterrence in Online Life. WebSci Conference 11, Koblenz, Germany.

Feigenbaum, J., A. D. Jaggard, et al. (2011). Towards a Formal Model of Accountability. New Security Paradigms Workshop. CA, USA.

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

International Medical Informatics Association (2002). IMIA Code of ethics for health information professionals. I. M. I. Association.

Jagadeesan, R., A. Jeffrey, et al. (2009). Towards a Theory of Accountability and Audit Computer Security – ESORICS 2009. M. Backes and P. Ning, Springer Berlin / Heidelberg. **5789:** 152-167.

Kagal, L. and H. Abelson (2010). Access Control is an Inadequate Framework for Privacy Protection. W3C Privacy Workshop.

Kagal, L. and J. Pato (2010). "Preserving Privacy Based on Semantic Policy Tools." Security & Privacy, IEEE **8**(4): 25-30.

Kargupta, H., S. Datta, et al. (2003). On the privacy preserving properties of random data perturbation techniques. Data Mining, 2003. ICDM 2003. Third IEEE International Conference on.

Lampson, B. (2005). Accountability and Freedom.

Lampson, B. (2009). "Privacy and security: Usable security: how to get it." Commun. ACM **52**(11): 25-27.

Moreau, L., P. Groth, et al. (2008). "The provenance of electronic data." Commun. ACM **51**(4): 52-58.

National E-Health Transition Authority (2011). Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system.

ODRL Initiative. (2012). "ODRL V2.0 - Core Model - Working Draft." from http://www.w3.org/community/odrl/two/model/.

Pratt, W., K. Unruh, et al. (2006). "Personal health information management." Commun. ACM **49**(1): 51-55.

Sloan, R. H. and R. Warner (2010). "Developing Foundations for Accountability Systems: Informational Norms and Context-Sensitive Judgments." Annual Computer Security Applications Conference, Workshop on Governance of Technology, Information, and Policies, 2010.

Solove, D. J. (2008). "Understanding Privacy." Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008.

Sweeney, L. (2002). "Achieving k-anonymity privacy protection using generalization and suppression." Int. J. Uncertain. Fuzziness Knowl.-Based Syst. **10**(5): 571-588.

Weitzner, D. J., H. Abelson, et al. (2008). "Information accountability." Commun. ACM **51**(6): 82-87.

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