Privacy Oriented Access Control for Electronic Health Records

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

Renato Iannella
NEHTA
Brisbane, Australia
renato.iannella@nehta.gov.au

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

ABSTRACT
Security and privacy in electronic health record systems have been hindering the growth of e-health systems since their emergence. The development of policies that satisfy the security and privacy requirements of different stakeholders in healthcare has proven to be difficult. But, these requirements have to be met if the systems developed are to succeed in achieving their intended goals. Access control is a fundamental security barrier for securing data in healthcare information systems. In this paper we present an access control model for electronic health records. We address patient privacy requirements, confidentiality of private information and the need for flexible access for health professionals for electronic health records. We carefully combine three existing access control models and present a novel access control model for EHRs which satisfies requirements of electronic health records.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection - *access control*

General Terms
Algorithms, Security

Keywords
Access control, MAC, DAC, RBAC, privacy, security, electronic health records, EHR

1. INTRODUCTION
Security of electronic health records (eHR) is a critical aspect of e-health solutions. Many different solutions have been developed over the years but the questions still remains as to whether the data in eHRs are secure enough. The National e-health transition authority (NEHTA) is the Australian authority dedicated to developing better ways of electronically collecting and securely exchanging health information. In their newest venture, the development of the personally controlled electronic health record (PCEHR) system, they have identified that privacy and security are major issues that need to be addressed properly in order for the proposed model to be well received [1]. Authentication is the initial stage of validation of the users to determine whether they are who they claim they are. Once authenticated, the users can enter an information system but access to information will still be governed by an access control policy. Access control is one of the main safeguards against improper data access. Access control aims to control the data usage of authorised users [2]. Access control models assume that the users are authorised to access the information system. After authorisation, the access control mechanism will define what information each authorised user can access. Many different access control models have been proposed and among them discretionary access control (DAC), mandatory access control (MAC) and role based access control (RBAC) are well established models.

Proper access control policies are a necessity for any EHR systems operation [1, 3]. Healthcare is an information dependant industry. The nature of the healthcare industry makes the access requirements different from other types of industries. Healthcare providers have data access requirements and the patients have data privacy requirements which may, in some instances, contradict the access requirements of the healthcare provider. Fulfilling all requirements is a complex task that has to be overcome in order to gain the confidence and trust of the end users of healthcare information systems.

In this paper we will introduce a privacy oriented access control model for electronic health records. The model is designed by combining the afore mentioned access control models with a purpose based access control (PBAC) mechanism for data access by authorised users. The purpose of the introduced access control model is to capture the different requirements of e-health into one module that can be adopted in a working electronic health records system.

2. RELATED WORK
In this section we will briefly introduce the access control models that have been considered in this paper. Even though these models have gone through many alterations and extensions, we will consider the basic principles behind each model so that is it easy to clarify how each model has been applied in our proposed access control model. Different access control strategies for e-health systems have also been developed in the past [3, 4]. Even though this work has been considered in developing the proposed model, due to space restrictions we will not discuss those techniques and approaches in this paper.

2.1 Discretionary access control
Discretionary Access Control uses access restriction set by the owner of the data object to restrict access to the objects. The

DUMW2012, April 16, 2012, Lyon, France.

users are bound by the authorizations which specify the operations each user can perform on specified objects such as read (R), write (W) and execute (EXE) [2]. The DAC model uses an access control matrix to assign access rights to users. A simple access control matrix is shown in Table 1.

Table 1. Access control matrix

User	Object 1	Object 2	Object 3	Object 4
Peter	R,W, EXE	R,W	-	R,W, EXE
Claudia	R,W	-	R,W, EXE	-
Bill	-	R,W, EXE	R, W	-
Matt	-	-	-	R,W, EXE

Implementing this matrix in large systems is a tedious task and representing it as a matrix will consume a considerable amount of resources. To represent this in a practical system the most common approach is by means of an Access Control List (ACL) and a Capability List (CL). An ACL is used to associate each object with the users who can access it. This association also contains the type of access (R, W, and EXE) to the object. This is a column wise representation of the access matrix. A Capability List is used to associate each user with the access permissions to the objects. This is a row wise representation of the access matrix.

DAC models have some inherent drawbacks. A significant issue is the fact that a user who is allowed to access an object by the owner of the object has the capability to pass on the access right to other users without the involvement of the owner of the object. This will create inevitable privacy issues if the DAC policy is used in an eHR system. Another factor we have to consider is the ownership of the data. In healthcare we cannot clearly identify a single entity as the owner of health data. An initial argument would be that the patients are the owners of their own health data. But patients are not always health professionals and it is likely that the involvement of a health authority of a relevant sort is necessary. Due to these reasons it is difficult to use only a DAC policy and fulfill access and privacy requirements of all healthcare stakeholders.

2.2 Mandatory access control

Mandatory access control systems do not consider the requirements of the owners of the data objects [5]. The access to data objects is controlled by assigning a security level to each object and comparing that security level to the user's security clearance and need-to-know. In order to access an object, the user must possess a clearance that is greater than or equal to the objects classification. In the MAC policy the flow of information from a higher security level to a lower security level is prevented by the "*Read Down*" and "*Write Up*" rules [2]. Similarly the integrity of the data objects can be protected by using the "*Read Up*" and "*Write Down*" Rules.

In a healthcare environment, we believe that assigning security levels to objects for the purpose of restricting access is not suitable. This is because the same type of data may have different sensitivity levels for different patients. We will discuss how we overcome this later in the paper.

2.3 Role based access control

Role base access control [6] models use permissions and rights that are assigned to roles in an organization to control access to data objects. It does not consider the access rights of an individual. Roles are assigned to all individual users in the systems. The users inherit the access permissions assigned to each role. This allows the system administrators to assign users to roles rather than go through the tedious task of assigning access rights to each and every user.

Roles are assigned to users depending on their capabilities and the job requirements within an organization. Each user must be given the least privilege depending on their job functions. RBAC policy uses the *need-to-know* principle to assign permissions to roles and to fulfill the least privilege condition.

2.4 Purpose based access control

According to the OECD guidelines, "*the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose*" [7]. Purpose-based access control (PBAC) is bases on the notion of relating data objects with purposes [8]. These purposes can determine for what reason data is collected and what they can be used for. Much research has been done in this area and most have identified that greater privacy preservation is possible by assigning objects with purposes [8-10]. However, according to Al-Fedaghi [11], purpose management introduces a great deal of complexity at the access control level. Despite the complexity issues with PBAC, it can help capture the reasons for data collection as well as the intentions of the users, which is a vital factor in healthcare information systems where privacy preservation is a must.

3. ACCESS AND PRIVACY REQUIREMENTS OF EHE END USERS

Environments such as healthcare require security mechanisms that are different and more specialized than those applicable to other industries. Access control models that have been developed are insufficient to fulfill the requirements of eHR systems [12]. This is due to the convoluted nature of the industry and the nature of the information used. To address this issue a specialized access control model has to be designed taking in to consideration the different requirements of different users/entities involved.

In healthcare there are certain requirements that cannot be disregarded when developing an information system. In this section we will discuss those requirements with respect to healthcare providers and patients that have to be considered and addressed in terms of access control.

3.1 Access Requirements of Healthcare Providers

The following access requirements of healthcare providers (both individual and the health authority) can be identified that need to be addressed in the development of an information system.

1. A healthcare authority should have the capability to define their security policies within an organization.
2. Healthcare providers need easy access to the relevant information in a non restrictive and timely manner.
3. Healthcare providers need to have the capability to share patient health information with other health specialists to make well informed decisions.
4. A healthcare authority should have the power to override the patients' security settings in certain

circumstances. E.g. A life threatening emergency situation.

3.2 Privacy Requirements of a Patient

A patient's health information may contain sensitive information such as sexual health, mental health, addictions to drug or alcohol, abortions, etc. This makes such a patient demand strong security for their eHRs. These requirements however cannot contradict those set by the healthcare providers or the healthcare authority discussed above. If they do so the settings set by the health authority must prevail. A formal definition of this is given later in the paper. We note however, that in the PCEHR [1] system proposed by NEHTA, all privacy settings are set by the patients. Therefore such conflicts will not arise in their proposed system. The following capabilities can be identified as requirements of a patient with an eHR in terms of access control.

1. Patients need to have the capability to control access to their eHR. They should be able to allow only a preferred set of medical practitioners to access their eHR.
2. Patients need to be able to hide certain health information from health practitioners who already have access to their eHR.
3. Patients need to have the capability to see how their eHR is manipulated by users who have access to it.
4. The administration process of the security settings must be easy to understand and handle.

It is important to note that access restrictions might not always be beneficial to the patient. While fulfilling these privacy requirements under no circumstance must the patients' health be compromised.

4. PROPOSED ACCESS CONTROL MODEL

The proposed model consists of four modules, a RBAC module, a MAC module, a DAC module and a PBAC module to fulfill the requirements of each of the stakeholders. The basic protocol for the proposed access control system is illustrated in Figure 1. We assume that the patient has a comprehensive eHR which is managed by a relevant health authority. In reality individuals may not want all information entered in to their eHR [1]. This requirement of course can easily be considered at the point of data entry. Nonetheless, we will show how a proper access control mechanism would eliminate the need to withhold information. In the proposed model the patient, the preferred healthcare providers and the health authority has certain operations and responsibilities to perform and fulfill.

Table 2. Data types and purposes

Data type	*Intended Purpose(s)*
Identity Data (PII)	p1
General Health	p1, p2, p3, p4
Sexual Health	p5
Mental Health	p5, p6, p7

The eHR is divided into data types (Table 2). Each data type in the eHR has to have a purpose or a set of related purposes. These are the intended purposes for which data is collected.

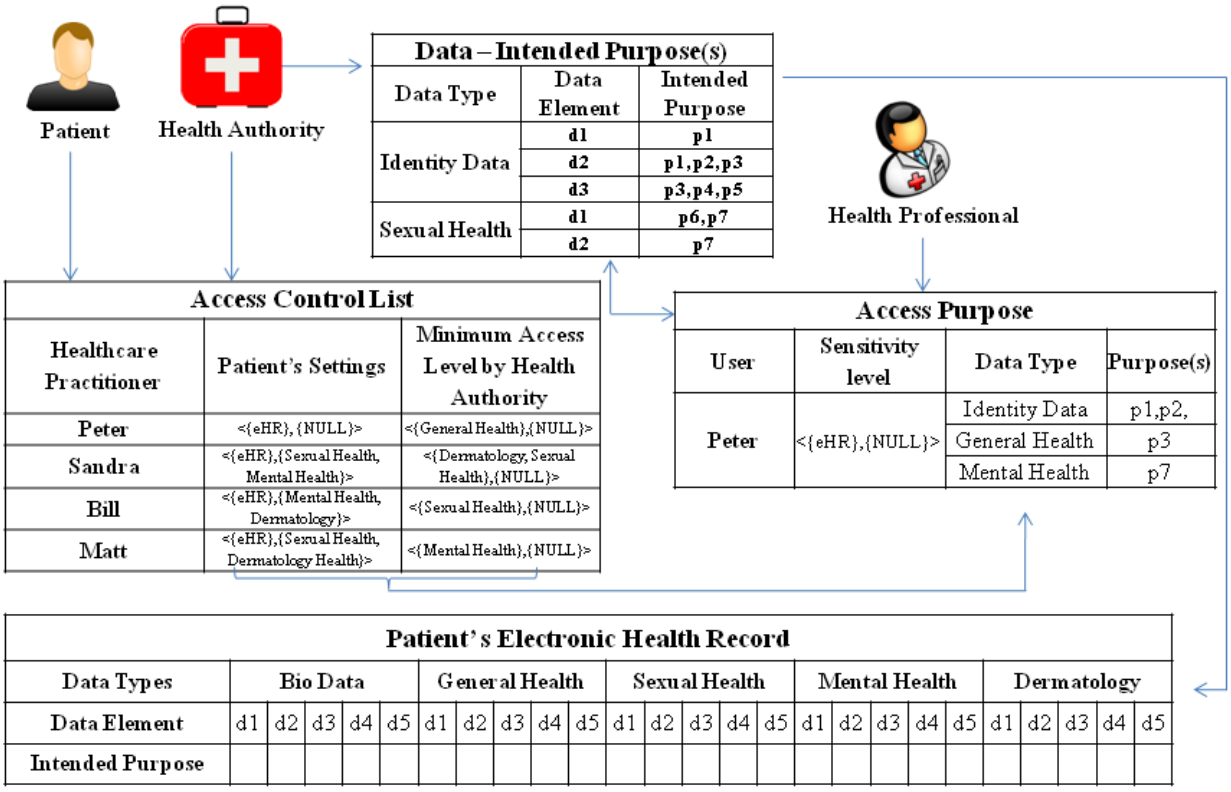

Figure 1. Proposed access control architecture

Definition of purposes, without doubt, is a complicated task that requires much care. This process itself has to explore medical knowledge from medical professionals who can identify the significance of a single data element in the care giving process. Purpose definition itself has to be a system design phase since these purposes will govern the final access to data in the proposed access control model. The data types contain data elements related to them. In a more fine grained level purposes are related to data elements. For example, Identity Data of a patient can be divided into Name, Date of Birth, Age, Residential Address, etc. The Address can be further divided into street address, Town, State, Country and post code. The more detached the data field gets, the more fine grained it become. We will not go into details of how each data element is related to purposes in this paper. We shall leave that under future work and will simply assume that sufficient relationships exist between data elements and purposes.

The health authority will manage the relationship between data types and purposes. There will be a default set of purposes for every data type and elements of that data type. The health authority can define, add and remove purposes related to data types and elements. This will ensure that up to date purposes are maintained in the systems such that the access requirements of care providers are not wrongfully denied. It is understood that the proper definition of intended purposes is a key factor in this model. For the system to reach an optimum performance level it will undoubtedly take time in which initial purpose definitions would be altered and new purposes defined. The data elements in the eHR are also assigned a sensitivity label. This label will be used to determine who has clearance to access the data element. The overall description of the proposed protocol is given in the sections below using a case scenario.

4.1 Case scenario

Gary has a comprehensive eHR which is managed by a central healthcare authority.

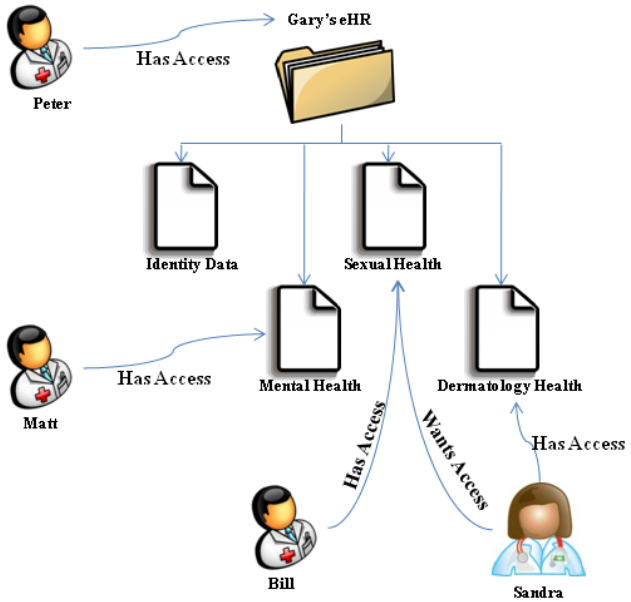

Figure 2. Case scenario

Gary's GP is Peter. As his GP, Gary has allowed Peter complete access to the data in his eHR. Gary has also been treated by Sandra a dermatologist, Bill a sexual health specialist and Matt a mental health specialist in the recent past. As a result Gary allows Bill to access his sexual health details, Matt to access his mental health details and Sandra to access his dermatology health details. He does not want Bill or Sandra accessing his mental health details and Matt or Sandra accessing his sexual health details. Gary suffers from a severe skin disease and does not want either Bill or Matt accessing his dermatology details due to embarrassment. He is aware that his care providers may need to share his information with other specialists but does not want them sharing the details without his consent. Sandra believes Gary's skin condition may be related to a known STD and wants access to Gary's sexual health details.

4.2 Role Based Access Control Module

In the RBAC module the healthcare authority will define the role structure of the health organization and assign the minimum access level for each role in the organization. In this role definition each role will be given a default sensitivity level for data access which will be discussed later. Even though the patients' privacy requirements have to be considered before data access is granted, there is no input from the patient for this module. The module is purely dedicated to fulfilling the organizational access and policy requirements. In a normal RBAC model, the role of the users has to change when the permissions for user changes. For this reason only the initial user-role assignment is done using the RBAC module.

4.3 Mandatory Access Control Module

In the MAC module, the health authority defines intended purposes for each data type and element. Deciding the sensitivity level of health information is a complex issue. The sensitivity labeling mentioned here are different from the classical hierarchical security levels found in MAC [2]. It is difficult to define a clear hierarchical structure for the sensitivity of data elements that is general to all participants. For example, sexual health and mental health information may have the same sensitivity label for some patients and may not be so for others. If a hierarchical structure is defined, it would be difficult to fulfill certain privacy requirements of patients.

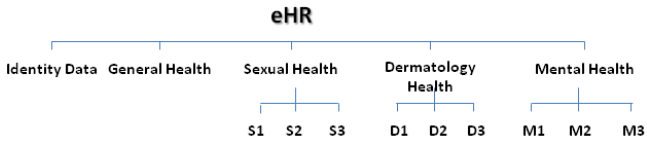

Figure 3. Object sensitivity tree

We propose sensitivity labeling of eHR data using a tree structure (Figure 3) that has the eHR itself as the root element, the data types as children and data elements as grandchildren. We use a similar technique introduced for purpose representation in Byun et al [13] to represent the sensitivity label of data elements in our model. We refer to this representation as the Sensitivity Tree (ST). A sensitivity label is not assigned to the objects themselves rather we relate the access level of a particular user in terms of the sensitivity label of the data elements.

Definition: A sensitivity label (SL) is a tuple <ASL, PSL>, where ASL = $\{asl_1, asl_2 \ldots asl_n\}$ a set of allowed sensitivity labels and PSL = $\{psl_1, psl_2 \ldots psl_n\}$ is a set of prohibited sensitivity labels.

ASL = $\{asl_i\}$; i = 1…n is denoted as all of the descendants of asl_i including asl_i.

$PSL = \{psl_j\}$; $j = 1 \ldots n$ is denoted as all of the descendants of psl_j including psl_j.

Example: Matt can access to Gary's mental health details but cannot access his Sexual or Dermatology details. The access level for Matt can be represented in terms of sensitivity labels as follows.

$SL_{Matt} = <\{eHR\}, \{Sexual\ Health, Dermatology\ Health\}>$

Here we use the Denial-Takes-Precedence [14] principle. Access is granted to the entire eHR and then access is denied to specific field by the PSL. This helps isolate the most sensitive information in the eHR that need to be hidden from certain users. The access level for a particular user can also be represented as follows.

$SL_{Matt} = <\{Identity\ Data, General\ Health, Mental\ Health\}, \{NULL\}>$

Specifying the data elements that Matt can access can be a tedious task than specifying the data elements he cannot access. We will use this representation to represent the minimum access levels defined by the health authority. The health authority is only concerned with allowing access to particular data fields for the relevant health practitioners. This representation can also be used in purposes such as research where access is required only to a particular data type.

Example: Data of a survey of people who have suffered from some form of a STD during the last 10 years. For this purpose access is required only for the sexual health data type. Under no foreseeable circumstance would there be a requirement for accessing other fields of the eHR. The access level can be represented as follows.

$SL_{Researcher} = <\{Sexual\ Health\}, \{NULL\}>$

Using this method of representing the access levels give enables more fine grained control over the data accessed by users.

4.4 Discretionary Access Control Module

In the DAC module the patient will specify who can access his eHR. He will populate an Access Control List (ACL) with the healthcare practitioners who he prefers to be able to access his eHR. The patient also has the capability to specify the access level of each of the users in terms of a sensitivity label in the ACL which is done using the MAC module as seen earlier.

Table 3. Access control list

Healthcare Practitioner	Patient's Settings	Minimum Access Level Set by Health Authority
Peter	<{eHR}, {NULL}>	<{General Health},{NULL}>
Sandra	<{eHR},{Sexual Health, Mental Health}>	<{Dermatology, Sexual Health},{NULL}>
Bill	<{eHR},{Mental Health, Dermatology}>	<{General Health, Sexual Health},{NULL}>
Matt	<{eHR},{Sexual Health, Dermatology Health}>	<{General Health, Mental Health},{NULL}>

The table above shows an abstract ACL. Gary has granted 4 health care practitioners access to his eHR. But the access is bound by the patient's privacy settings and the settings by the health authority. The settings by the health authority are set during the role assignment in the RBAC module.

The sensitivity level defined by the health authority is different to what is defined by the patients. PSLs set by the health authority will always be *NULL*. As mentioned above, this is because the health authority is concerned with allowing access to the health professionals. The prohibitions are defined by the patients. The allowed sensitivity level set by the patients always precedes that which is set by the health authority if there is no conflict between the patients prohibited sensitivity label and the allowed sensitivity label set by the health authority. The allowed sensitivity level set by the health authority always precedes the prohibited sensitivity label set by the patients if there is a conflict. This characteristic/notion will ensure that the relevant information is always available to the right person in terms of providing better healthcare. A formal definition for this notion is given below.

Definition:

- IF ($ASL_{Patient} \geq ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} = \emptyset$) THEN $SL_{HealthProfessional} = <\{ASL_{Patient}, \{PSL_{Patient}\}>$
- IF ($ASL_{Patient} \leq ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} = \emptyset$) THEN $SL_{HealthProfessional} = <\{ASL_{HealthAuthority}\}, \{PSL_{Patient}\}>$
- IF ($ASL_{Patient} \geq ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} \neq \emptyset$) THEN $SL_{HealthProfessional} = <\{ASL_{Patient}\}, \{PSL_{Patient} \cap ASL_{HealthAuthority}`\}>$

When these conditions are satisfied, the sensitivity levels are updated so that the users can access the relevant data types/elements. E.g. Sandra (Table 4) will be assigned a sensitivity level $SL_{Sandra} = <\{eHR\}, \{Mental\ Health\}>$.

Algorithm 1 shows how sensitivity levels are set for the users. The symbols other than the ones used previously denote as follows. P_{SL} and HA_{SL} denote sensitivity levels set by the Patient (*P*) and the Health Authority (*HA*) respectively.

Algorithm 1: Set Sensitivity Label SL_{UID}

Input: 1. User ID: *UID*
2. Access Control List: *ACL*
Output: User Sensitivity Label SL_{UID}
Method:
  $P_{SL\_UID} \leftarrow <ASL_{P\_UID}, PSL_{P\_UID}>$
  $HA_{SL\_UID} \leftarrow <ASL_{HA\_UID}, PSL_{HA\_UID}>$
  if ($ASL_{P\_UID} \geq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} = \emptyset$) **then**
    $SL_{UID} \leftarrow <\{ASL_{P\_UID}\}, \{PSL_{P\_UID}\}>$
    else if ($ASL_{P\_UID} \leq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} = \emptyset$) **then**
      $SL_{UID} \leftarrow <\{ASL_{HA\_UID}\}, \{PSL_{P\_UID}\}>$
    else if ($ASL_{P\_UID} \geq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} \neq \emptyset$) **then**
      $SL_{UID} \leftarrow <\{ASL_{P\_UID}\}, \{PSL_{P\_UID} \cap ASL_{HA\_UID}`\}>$
    else if ($ASL_{P\_UID} \leq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} \neq \emptyset$) **then**
      $SL_{UID} \leftarrow <\{ASL_{HA\_UID}\}, \{PSL_{P\_UID} \cap ASL_{HA\_UID}`\}>$
  end if
  return SL_{UID}

4.5 Purpose Based Access Control Module

This module primarily deals with the access requests of authorised users. When a user requires access to data in an eHR they define an access request consisting the reason(s) or purpose(s). This definition will be compared to the purposes in Table 2 which were assigned to the data elements by the health authority and if satisfied access will be granted.

Table 4 represents typical access requests by authorised health practitioners. An access request may not particularly be for a single task. And each data type requested may not always be associated with a single purpose. The users must have the capability to specify multiple purposes in a single access request to enhance the ease of use. If access is granted we have to make the assumption that each data element can only be used for the specified access purpose(s). The health information systems which would use this access control model should have the capability to provide the functionality where data misuse can be captured.

Algorithm 2: Access Request

```
1:  Input:  1. User ID: UID
2:          2. Sensitivity Level: SL_UID
3:          3. Access Purposes List: AccPurList[d_AP, p_AP]
4:          4. Access Control List: ACL
5:          5. Intended Purposes List: IntPurList [d_IP, p_IP]
6:  Output: Access_State []
7:  Method:
8:   Num_Requests ← Size (AccPurList)
9:   Access_State [Num_Requests] ← False
10:  Permit_Data [Num_Requests] ← False
11:  Check_Purpose [Num_Requests, Num_Pur] ← False
12:      for i = 1 to Num_Requests do
13:              if IntPurList(i) ∈ PSL(SL_UID) then
14:                      Permit_Data[i] ← False
15:              else
16:                      Permit_Data[i] ← True
17:               end if
18:      for j = 1 to Size(AccPurList(i)) do
19:              if AccPurList[i, j] ⊆ IntPurList then
20:                      Check_Purpose [i, j] ← True
21:              else
22:                      Check_Purpose [i, j] ← False
23:              if {(Permit_Data [i] = True) AND
         (Check_Purpose [i, j] = True ) = True} then
23:                      Access_State [i] ← True
24:              else
25:                      Access_State [i] ← False
26:              end if
27:      end for
28:      end for
29:      return Access_State []
```

Algorithm 2 processes the access requests by health professionals. A tuple with data type and purpose is denoted as *<d, p>*. *Permit_Data []* contains the status (allowed or disallowed) of the data types requested by the user. *Check_Purpose [Num_Requests, Num_Pur]* is a 2D array containing the status of the purposes for each the data type requested. The algorithm returns and array *Access_State []* with the state of each purpose in the access request. *IntPurList* $[d_{IP}, p_{IP}]$ is a 2D array with data types with their intended purposes (set by the health authority). *AccPurList* $[d_{IP}, p_{IP}]$ is a 2D array with the data types and their access purposes (requested by a user)

Table 4. Access requests by authorised users

User	*Sensitivity level*	*Data Type (d)*	*Access Purpose (p)*
Peter	<{eHR},{NULL}>	Identity Data	p1,p2
		General Health	p3
		Mental Health	p7, p4
		Sexual Health	p5
Sandra	<{eHR},{Mental Health}>	Dermatology	p8
		Sexual Health	p5

It is important to note that the nature of the healthcare industry force us to adopt the *break the glass* emergency mechanisms where the patients health prevails over privacy requirements. Also, usability is a vital part of every healthcare information system. No matter what the underlying principles are, the users, both patients and the healthcare providers must be given simple directions (e.g. menu) where they can set their access settings easily.

4.6 Information Sharing Example

In our case scenario let us assume that Peter, using the PBAC module defined within the portal for authorised users, initiates a request to share Gary's sexual health details with another health professional Claudia for the benefit of Gary. Here however, Claudia should have the relevant access clearance by the health authority to access the type of data specified by the requester. This default access level is set using the RBAC and MAC modules of the access control model. It is not necessarily required that the receiving health professional be in Gary's ACL which is defined by Gary through the DAC and MAC modules since it is a request by an authenticated user. It is important to note that Gary's consent for sharing information is already given to Peter by the policies set by the patient and the health authority. Gary can give any health professional the right to share his health information without his consent with other health professionals. If Claudia accepts the request she becomes an authorised user of the system with the relevant access level. Gary has the right to remove Claudia from the ACL at a later time. Gary is notified of the actions of the users at relevant times to make the system transparent. It is important to note that information is shared for the benefit of the patient. Information must not be misused by the users. Trust plays a major role in the information sharing process. Furthermore, such processes are traceable and accountable. An eHR system using this protocol must have the capability to prevent users from misusing information.

5. PROTOTYPE

A prototype of the proposed access control model was developed. The prototype is a Web based system aimed at testing the proposed protocol. A Web based prototype was developed because with extensions, information accountability systems with reasoning capabilities such as the one proposed by Gajanayake et. al [15] can be developed.

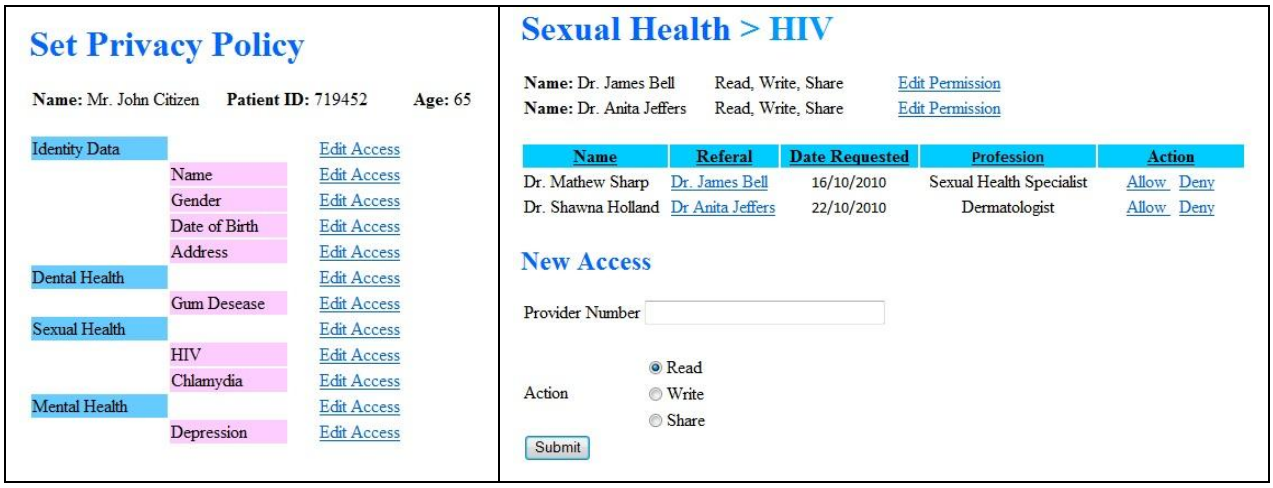

Figure 3. Left: patients can allow or deny access to data types for health professionals Right: patients can view current health professionals who has access to particular data elements and can assign new health professionals to access the data elements

This implementation is focused only on demonstrating the proposed access control protocol. We are not focused on actual system usability at this stage. Figure 3 shows a portion of the prototype that allows patients to set and manage their privacy policies.

The prototype is developed to handle three types of users; patients, health authority and health professionals. The patients and the health authority can set privacy and access policies and the final policies are formulated according to the protocol discussed above. A simple SQL database is used to hold the policies and the data in the eHR. Health professionals can lodge access requests which consist of access purposes and will be processed according to the protocol using an intended purposes database managed by the health authority. The management of intended purposes is not facilitated in this prototype.

6. DISCUSSION

Access control has been a fundamental security measure of information systems for many years. Amongst many different models DAC, MAC, RBAC and PBAC are the most popular. These models come in many different variations and are used in different contextual domains. In this paper we discussed how we can make use of the characteristics and principles of these models to facilitate a suitable access control model for electronic health records. We identified specific requirements of different healthcare stakeholders and combined the principles behind the DAC, MAC, RBAC and PBAC models to address them. The DAC model is used to capture the access settings for users by patients. Patients maintain an ACL of their trusted health professionals and use a variation of the MAC model to assign access levels (or sensitivity level as discussed above) for them. The MAC model is used to define access levels of health professionals who can access data in an eHR. A central health authority uses a RBAC model and the MAC model to set default access levels for health professionals. A simple PBAC model is used as a usage control module to capture the access purposes of information users. The current prototype is capable of demonstrating the process of setting the access levels by the patients and the health authority and processing access requests by health professionals. We have tested the prototype to demonstrate various scenarios of policy settings and data access. Further development and testing is required to investigate how this model would behave in the complex domain of healthcare. Rather than being used as a standalone security model, the final goal of our research is to harmonize the access control model with an information accountability framework (IAF) for e-health. The IAF uses DRM technologies to represent the access and usage policies set by the users in a Rights Expression Language [16].

7. CONCLUSION AND FUTURE WORK

In this paper we have introduced a novel access control model for electronic health record systems using prominent access control models. We have identified certain requirements of end users of an electronic health record system and our proposed model is designed to fulfill those requirements. Further to what has been discussed in this paper we propose the following additions. Purpose definition is an important part in our model. Building a comprehensive set of purposes and maintaining them is vital. These definitions must capture medical knowledge as well as system requirements. The health details of family members and relatives are an important resource that must be available to the caring professional. We intend to extend the proposed model such that those links can also be incorporated in to the model while still maintaining the integrity of the privacy capability of the model. We are also working to extend the proposed model to support explicit actions as described in [17] and providing non-restrictive access to health information for the authorized persons while incorporating an information accountability framework [15] so that health information would not be misused. Proper representation of policies is vital for such systems. We have extended the proposed access control model such that the policies are represented in a suitable rights expression language, namely the open digital rights language (ODRL) [18]. In this extended work we introduce an information accountability framework with policy reasoning capabilities which adheres to information accountability principles.

8. ACKNOWLEDGEMENTS

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

9. REFERENCES

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

[2] Sandhu, R. S. and Samarati, P. Access control: principle and practice. *Communications Magazine, IEEE*, 32, 9 1994), 40-48.

[3] Motta, G. H. M. B. and Furuie, S. S. A contextual role-based access control authorization model for electronic patient record. *Information Technology in Biomedicine, IEEE Transactions on*, 7, 3 2003), 202-207.

[4] Alhaqbani, B. and Fidge, C. Access control requirements for processing electronic health records. In *Proceedings of the Proceedings of the 2007 international conference on Business process management* (Brisbane, Australia, 2008). Springer-Verlag.

[5] Ferraiolo, D., Kuhn, D. R. and Chandramouli, R. *Role-based access control*. Artech House, 2003.

[6] Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman, C. E. Role-based access control models. *Computer*, 29, 2 1996), 38-47.

[7] OECD *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. City, 1980.

[8] Byun, J.-W., Bertino, E. and Li, N. Purpose based access control of complex data for privacy protection. In *Proceedings of the Proceedings of the tenth ACM symposium on Access control models and technologies* (Stockholm, Sweden, 2005).

[9] Naikuo, Y., Howard, B. and Ning, Z. *A Purpose-Based Access Control Model*. City, 2007.

[10] Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J. and Trombetta, A. Privacy-aware role-based access control. *ACM Trans. Inf. Syst. Secur.*, 13, 3 2010), 1-31.

[11] Al-Fedaghi, S. S. Beyond purpose-based privacy access control. In *Proceedings of the Proceedings of the eighteenth conference on Australasian database - Volume 63* (Ballarat, Victoria, Australia, 2007). Australian Computer Society, Inc.

[12] Finance, B., Medjdoub, S. and Pucheral, P. *Privacy of medical records: from law principles to practice*. City, 2005.

[13] Byun, J.-W. and Li, N. Purpose based access control for privacy protection in relational database systems. *The VLDB Journal*, 17, 4 2008), 603-619.

[14] Bertino, E. Data security. *Data & Knowledge Engineering*, 25, 1-2 1998), 199-216.

[15] Gajanayake, R., Iannella, R. and Sahama, T. Sharing with Care: An Information Accountability Perspective. *Internet Computing, IEEE*, 15, 4 2011), 31-38.

[16] Gajanayake, R., Iannella, R. and Sahama, T. An Information Accountability Framework for Shared E-Health Policies. In *Proceedings of the Workshop on Data Usage Management on the Web* (Lyon, France, 2012).

[17] HL7 *Role Based Access Control (RBAC) Role Engineering Overview*. City, 2010.

[18] ODRL Initiative *ODRL V2.0 - Core Model - Working Draft*. City, 2012.