AN XACML BASED FRAMEWORK FOR STRUCTURED PATIENT PRIVACY POLICY (S3P)

A THESIS SUBMITED TO
THE GRADUATE SCHOOL OF INFORMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

MEHRDAD ALIZADEH MIZANI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF MEDICAL INFORMATICS

SEPTEMBER 2006

Approval of the Graduate School of Informatics

_____

Assoc. Prof. Dr. Nazife BAYKAL
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assist. Prof. Dr. Erkan MUMCUOĞLU
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Nazife BAYKAL
Supervisor

Examining Committee Members

Prof. Dr. Aydan ERKMEN (METU, EEE) _____

Assoc. Prof. Dr. Nazife BAYKAL (METU, IS)_____

Prof. Dr. İbrahim BARIŞTA (Hacettepe U.)_____

Assist. Prof. Dr. Didem GÖKÇAY (METU, MIN)_____

Assist. Prof. Dr. Erkan MUMCUOĞLU (METU, IS) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this wok.

Name, Last name : Mehrdad, Alizadeh Mizani

Signature : _____

ABSTRACT

AN XACML BASED FRAMEWORK FOR
STRUCTURED PATIENT PRIVACY POLICY (S3P)

Mehrdad Alizadeh Mizani
M.Sc., Department of Medical Informatics
Supervisor: Assoc. Prof. Dr. Nazife Baykal

September 2006, 109 pages

The emergence of electronic healthcare have caused numerous changes in both substantive and procedural aspects of healthcare processes. Such changes have introduced new risks to patient privacy and information confidentiality. Traditional privacy policies fall too short to respond to privacy needs of patients in electronic healthcare. Structured and enforceable policies are needed in order to protect patient privacy in modern healthcare with its cross organizational information sharing and decision making. Structured Patient Privacy Policy (S3P) is a framework for a formalized and enforceable privacy policy in healthcare. S3P contains a prototype implementation of a structured and enforceable privacy policy based on eXtensible Access Control Markup Language (XACML). By simulating healthcare scenarios, S3P provides a means for experts from different professional backgrounds to assess

the effect of policies on healthcare processes and to reach ethically sound privacy policies suitable for electronic healthcare.

Keywords: Patient privacy policy, XACML, Policy enforcement, Structured policy, Privacy policy framework

ÖZ

XACML TABANLI YAPILANDIRILMIŞ HASTA MAHREMIYETI POLIÇESI (YHMP) SISTEMI

Mehrdad Alizadeh Mizani
Yüksek Lisans, Sağlık Bilşimi
Tez Yöneticisi: Doç. Dr. Nazife Baykal

Eylül 2006, 109 sayfa

Elektronik sağlık hizmetleri sağlık süreçlerinin hem temel özelliklerinde hem de süreçlerinde bir çok değişikliğe neden olmuştur. Bu değişiklikler hasta mahremiyeti ve bilginin gizliliğini de tehdit eden riskleri de beraberinde getirmiştir. Elektronik sağlık hizmetlerinde geleneksel gizlilik poliçeleri hastaların mahremiyetini korumada yetersiz kalmaktadır. Yapılandırılmış ve uygulanabilir poliçeler, bir çok organizasyonun bilgi paylaşımına ve karar verme süreçlerine katıldığı modern sağlık hizmetlerinde gereksinim duyulan hasta mahremiyetini korumada gerekli olmaktadır. Yapılandırılmış Hasta Mahremiyeti Poliçesi (YHMP) sağlıkta biçimlendirilmiş ve uygulanabilir bir gizlilik poliçesi sistemidir. YHMP, eXtensible Access Control Markup Language (XACML) tabanlı yapılandırılmış ve uygulanabilir gizlilik poliçeleri içeren bir prototip uygulamasına sahiptir. Sağlık

hizmetleri senaryolarını benzetimleyen YHMP, farklı mesleki geçmişlerden gelen uzmanların sağlık hizmetleri süreçlerine etki eden poliçelerin etik olarak uygun olup olmadığını sınamasına olanak tanımaktadır.

Anahtar kelimeler: Hasta mahremiyeti poliçesi, XACML, polıçe uygulanması, biçimlendirilmiş poliçe, gizlilik poliçesi sistemi

ACKNOWLEDGMENTS

I am greatly appreciative to my advisor Assoc. Prof. Dr. Nazife Baykal for her guidance and support throughout my study. I am also grateful to my thesis committee for their suggestions and valuable comments.

I would like to express my deepest gratitude to my parents and sister who always encouraged me with their love, understanding, patience, and emotional support. They always gave me the courage and strength I needed to achieve my goals.

I would like to express my sincere appreciation to Dr. Arda Arıkan, who endured this long process with me, for his helpful suggestions and continuous moral support.

I also thank to my friend Oya Deniz Koçgil for her useful comments, discussions, and encouragements throughout my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
CCR	Continuity of Care Record
EHR	Electronic Health Record
EPAL	Enterprise Privacy Authorization Language
HCO	Health Care Organization
HIPAA	Health Insurance Portability and Accountability Act
OASIS	Organization for the Advancement of Structured Information Standards
P3P	Platform for Privacy Preferences Project
PHI	Protected Health Information
S3P	Structured Patient Privacy Policy
UHI	Unique Health Identifier
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

CHAPTER 1

INTRODUCTION

1.1: Background to the study

Protecting patient privacy is an important and complex task. Privacy is a shared agreement with an ethical core dated back to Hippocrates[1]. Modern healthcare, with all its new aspects and diversity of parties, has compounded the privacy protection efforts. In the last three decades, technological innovations have changed the healthcare processes considerably. These changes have introduced new types of vulnerabilities and risks to all aspects of modern healthcare including privacy protection. It is not a trivial task to countermeasure the risks and vulnerabilities targeting the health information mainly because it is not easy to measure the risks in terms of human life [2].

New advancements, especially electronic health records (EHRs), have changed the substantial and procedural nature of healthcare processes. EHR makes medical information vulnerable to the threats targeting all types of electronic media. Electronic representation, use, and transmission of medical information have introduced new challenges in protecting the patient privacy. Additionally, the advancement of network technologies has facilitated cross organizational information sharing among different healthcare organizations. As a result, traditional healthcare, which was based on physician-patient relation, has changed into an organizational and collaborative shared care model in which various professions involve in care providing process. In modern shared care, several parties holding different moral values and potentially from different healthcare organizations, take part in decision making processes regarding a patient. On the other hand, in the modern right based society, patients have a right to take part in decision making processes regarding

them and claim their privacy rights.

"The emergence and evolution of a new technology gives us a chance to test old tools and, as necessary, to invent new ones in order to get better moral leverage on the problems at hand. Such tools will inform our decisions, guide our actions, and prepare us for future challenges." [3] Such tests and new inventions are necessary in privacy area as well. Privacy protection in traditional healthcare is mainly done by reaching a private agreement between physician and patient. However, in modern shared care there is a need for policies to regulate the actions of different parties involved. As Winkler argues [4], an organization wide policy which covers all individuals in health care organization (HCO) and deals with both standard and morally controversial medical practices ensures autonomy, quality, fairness, and efficiency of decision making processes. Although many HCOs have privacy policies which may be informed to patients, privacy violations still occur [5]. Privacy rules and regulations change frequently. Such changes do not always preserve the patient's rights. According to "National Consumer Health Privacy Survey 2005" [6], the implementation of health insurance portability and accountability act (HIPAA) in the United States has not reduced the consumers' concerns about their privacy. According to this study, about 67 percent of American respondents are "somewhat" or "very concerned" about the privacy of their private medical records. The sole presence of privacy policy and informing it to care providing individuals and patients does not necessarily guarantee the privacy protection. Here are some reasons of why most existing policies are not adequate to protect patient privacy:

- Dynamic nature of privacy protection: Protecting privacy is a process which requires the revision of policies in order to justify their ability to protect patient privacy. Policies may contain conflicts or hidden leaks because of diversity of parties and intersection of duties in healthcare. Existing policies are static entities mainly consisting of general guidelines. This makes the revising and changing the policy a costly, time consuming, and inefficient task.
- Authorized abuse: Unlike security policy which prevents the access of unauthorized users to protected assets, privacy policy involves with providing access to authorized users. Even a highly restrictive security policy in effect can not prevent the inadvertent or rarely intentional

"authorized abuse" [7], which is the inappropriate use or disclosure of information by authorized users.

- Awareness: There is a lack of awareness of privacy issues in many HCOs. Even patients are not fully aware of their rights. They often are willing to disclose their private information to others which makes privacy protection efforts inefficient.
- Lack of standards in policy sharing: In shared care, patient information is transmitted to another HCO for collaborative care. There could be different privacy protection measures in referring and referred HCOs. A more relaxed policy in the refereed HCO may lead to privacy violation, yet a more restrictive policy may cause the lack of availability of vital information. There is no agreed upon standard for policy representation and management in HCOs.
- Ambiguity: Policies are almost always represented in plain language which can lead to ambiguity of privacy rules or inappropriate interpretations. The informed consents reflecting the privacy policy to patients, are somehow vague in informing patients about the actual and possible uses of medical information.
- Lack of enforcement: The ambiguity of policy and the diversity of parties, may lead to decision making based on personal values, which may be in conflict with the policy or patient expectations. There is no way to guarantee that all parties conform to the policy or have a clear understanding of policy rules.

As a result, traditional privacy policies fall too short to respond to the emerging privacy requirements of electronic healthcare and patient expectations. Therefore, there is a need for new forms of policy management including:

- Structuring and standardizing the policy: To overcome the ambiguity of policy rules, there is a need to represent policy in a structured and standard way.
- Enforcing and automating the policy: Policies should be enforced to ensure the conformance of all parties and to provide accountability.

This enforcement and automation can be achieved by computerizing access control and decision making processes.

- Dynamic policies: Revising and changing the policies can be done more efficiently with structured policies. Automated policies can reflect the latest changes of the policy.

Structured Patient Privacy Policy (S3P) is a framework for a formalized and enforceable privacy policy in healthcare. Additionally, we have designed a prototype application covering the privacy policy concerning the access control for the primary uses of the health information. It is a JAVA based application which simulates a privacy policy based on eXtensible Access Control Markup Language (XACML). The access conrotl is based on role based access control (RBAC).

1.2: Purpose of the study

The purpose of designing and implementation of S3P is:

- To provide a framework for structured and enforceable patient privacy policies.
- To provide a simulation of automated patient privacy policy.
- To simulate a structured policy based on a standard language to assist further studies on interfacing policies between different HCOs.
- To provide a means for experts from different professional backgrounds to assess the effects of structured and enforceable privacy policies on healthcare processes.
- To provide a means to highlight the new aspects of privacy protection in electronic healthcare.
- To highlight the technical, procedural, and ethical problems of privacy protection in electronic healthcare to assist the experts to collaboratively find the most appropriate solutions.

1.3: Significance of the study

The importance of this study lies in its emphasis on practical simulation of structured policy through S3P application. S3P can be used to simulate real life like healthcare scenarios of electronic healthcare, hence, expanding the experiential knowledge of privacy protection. This can be helpful while bridging theory and practice, thus, enabling us to present ethically sound privacy policies. On the other hand, it can be used as an educational tool to assist its users to learn about various aspects of privacy issues in electronic healthcare. Additionally, this simulation can be helpful in highlighting potential problems and deficiencies in policies. Therefore, S3P can aid expert from different professional backgrounds to examine the policy practically. As a result of such examination, experts can collaboratively find the best technical, managerial, organizational, ethical, and legislative solutions.

CHAPTER 2

REVIEW OF CONCEPTS

2.1: Privacy policy

"Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves." [8] Privacy protection in traditional healthcare was mainly dependent on a simple agreement between patient and the physician. The physician was the main decision maker and the patient records was only accessible by few parties under the control of physician and patient. In modern healthcare, however, several parties from medical or non-medical backgrounds are involved in health care processes. For instance general practitioners, specialists, nurses, and insurance companies may have access to health records for a simple inpatient care providing. In shared care, several healthcare organizations share patient records across organization boundaries for shared decision making. Furthermore, researchers and third parties may be given access to patient records or parts thereof for research or marketing purposes. As a result, restricting the view to health records and controlling the flow of information becomes extremely complex comparing to traditional physician-patient healthcare model. Roy Rada [9] argues that establishing a relationship with a record-keeping organization causes the patients to lose some of the controls that they had in face-to-face relationships, and as a result, the patient faces challenges trying to :

- check on the accuracy of the information the organization develops.
- correct any errors that may exist in the information.
- know the full extent of uses of the information.

- know the disclosures of the information.
- sever the relationship with the organization.

Accurate record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice [10]:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

In order to provide adherence to aforementioned principles there is a need for enforcing information usage rules on care providers and to inform and and empower the patients. To regulate the action of all parties involved in care providing, and to accurately inform patients, organization wide policies are needed. Policy is defined in Merriam-Webster dictionary as "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions." [11] As for information systems, "A policy describes the legal framework including rules and regulations, the organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties defined as well as the technological solution implemented for collecting, recording, processing, and communicating data in information systems." [12] Healthcare organizations may have several types of policies, such as security policy and privacy policy. Unlike security policy which restricts the access of unauthorized users, privacy policy

mainly involves with regulating the actions of authorized users.

A privacy policy is a formal statement describing the legitimate uses and disclosures of health information (refer to appendix A). The two main functions of privacy policies are to regulate the actions of parties involved in healthcare and to inform the patients about the possible actions on their records (refer to 2.2). Furthermore, patients have a right to include or exclude specific uses or disclosures of their health records (refer to 2.3) from the policy. Figure 2 depicts the relationship of the privacy policy with health organization and with the patient. According to the American Civil Liberties Union (ACLU) believes, a privacy policy for health information should be based on the following principles [13, 14]:

- Strict limits on access and disclosure.
- Individual control over health records.
- Built-in security measures.
- Denial of access to employers.
- Notice to patients of all uses of medical records.
- Right of access to personal medical and financial records.
- Remedies for wrongful disclosure or misuse of information.
- Federal oversight to ensure compliance.

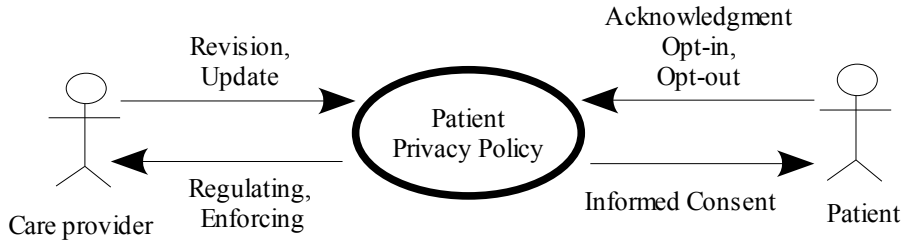

Figure 2-1: Relationship of the privacy policy with care providers and patients

2.2: Informed consent

Informed consent is an institution-wide notice describing the practices of the healthcare organization regarding patient health information in order to gather the

acknowledgment of patients or research subjects on their acceptance to inclusion in such practices [15, 16]. Informed consent contains all legitimate uses and disclosures of patient information. As for treatment or trial studies, it is generally accepted that complete informed consent includes a discussion of the following elements [17]:

- The nature of the decision/procedure.
- Reasonable alternatives to the proposed intervention.
- The relevant risks, benefits, and uncertainties related to each alternative.
- Assessment of patient understanding.
- The acceptance of the intervention by the patient.

Informed consent is usually informed to patients at their first visit to a health organization. Patients read and sign the consent if they accept it. Therefore, informed consent acts as a communication process between health provider and the patient [18]. Such communication helps preserving patient rights by facilitating the care providers' conformance to the following principles [19]:

- **Information Disclosure:** The right to receive accurate and easily understood information about the health plane and decisions.
- **Choice of Providers and Plans:** The right to choose health providers which provide the patients with access to appropriate high-quality health care.
- **Access to Emergency Services:** The right to receive emergency services whenever and wherever needed, without prior authorization or financial penalty.
- **Participation in Treatment Decisions:** The right to know all treatment options and to participate in decisions about one's care. The right to designate individuals as representatives for decision making when the patient cannot makes his or her own decision.
- **Respect and Nondiscrimination:** The right to considerate, respectful, and nondiscriminatory care from care providers.
- **Confidentiality of Health Information:** The right to talk in

confidence with health care providers and to have health care information protected. The right to review and copy one's own medical record and request that record keeping care providers amend health record if it is not accurate, relevant, or complete.

- **Complaints and Appeals:** The right to a fair, fast, and objective review of any compliant the patient has against the care providers.

Nevertheless, informed consent provides the patients with an informed decision about their relation with the healthcare organization, it introduces some problems in several cases, such as:

- The first visit of a patient who is not able to comprehend or acknowledge the consent, for instance due to unconsciousness.
- Patient disagreement to parts of the policy which are necessary for accurate care providing or the safety of patient or staff, such as restricting access to HIV status.
- Conflicts between physician moral values and patients acknowledged consents, such as decision making about blood transfusion to Jehovah witnesses [4].

In the final modification of HIPAA rule adopted on August 2002 [20], the mandatory consent replaced with voluntary contest in order to eliminate barriers of mandatory consent to care providing [21]. It can be seen in the same resource that "The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care."

2.3: Opt-in and Opt-out

As mentioned in sections 2.1 and 2.2, the privacy policy includes all legitimate uses and disclosures of health information and that such uses or disclosures are declared to patients through informed consent. Patients upon receiving the informed

consent are asked to sign an acknowledgment that they have read and accepted the privacy policy of the organization. There are two approaches to get patient acknowledgment:

- Opt-in: In which the patient is excluded of all information uses and disclosures activities by default. Patients need to explicitly accept and acknowledge their inclusion in any information gathering, usage or disclosure.
- Opt-out: In which the patient is included in all information uses and disclosure activities by default. Patients need to explicitly acknowledge their exclusion of any activity that they object to.

There is not consensus about the advantages of one approach to the other. "For example, while the EU Privacy Act requires that individuals explicitly consent to personal data collected by an organization being used for commercial purposes – opt-in – the US has almost the opposite approach. In the US there is less general legislation, and consent is generally implied unless the individual explicitly opts-out of such usage." [22]

There are advantages and disadvantages of both approaches. For example, Justin M. List [23] argues that opt-in for kidney donors contains an unnecessary level of discrimination in kidney allocation for those who do not opt-in. He additionally discusses three concerns of opt-in for kidney donors: enrollment dilemmas, decision making for minors, and fairness. In a comparison between opt-in and opt-out for prenatal screening for HIV infection, is is argued that the opt-out increases the testing rates, hence, decreases the mother-to-child HIV transmission [24, 25]. Sharon Walsmley also argues that resource that "a woman who receives a positive HIV test result may be faced with issues of discrimination and stigmatization associated with the diagnosis. ... Therefore, for optimal use of an opt-out approach, physicians must be certain that the objectives, risks and benefits of the strategy are explained to their patients and that the women understand their right to refusal." [24] Therefore, patient should be informed about their rights and about the consequences of their opt-in or opt-out option. Such patient awareness is necessary because studies show that even the way of questioning influences the patient options and that simply framing the questions as an opt-out instead of opt-in changes the privacy preferences [26 as cited in 27].

2.4: Unique Health Identifier

In many traditional healthcare organizations, personal identifiers, such as name and last name, are used to identify and retrieve patient information. Using personal information as patient identifier is endangers patient privacy and safety. Similar names and misspelling causes the retrieval the information of another patient. Such wrong record retrieval could have life threating consequences because vital information of the patient would not be accessible. Additionally, misspelling and failure to retrieve an existing patient record, may lead to issuing a new health record for that patient. Such duplication of records results in incomplete and incoherent health records which prevents the continuity of care. A combination of personal information as an identifier could reduce the aforementioned risks, yet searching via such combination of information is highly time consuming. HIPAA recognized the need for a unique individual identifier as part of the administrative simplification process [28].

Each healthcare organization may use a numerical or alphanumerical identifier to uniquely identify patient records. Although such identifiers uniquely identify a patient in a single healthcare organization, they are not effective in shared care. Patients may have records in several healthcare organizations with their health information scattered through various databases. To provide a high quality care and to promote continuity of care, patient record should be retrievable from all healthcare organizations. Access to such distributed health record requires an integrated and agreed upon way of identifying patient between different organizations. Using and managing different identifiers by healthcare organizations prevents such interoperability between care providers to unequally identify patients.

Other unique identifiers, such as social security number, are used in many organizations to uniquely identify patients. Obviously, such identifiers satisfy the unique identification of patients both in a single HCO and in shared care for primary uses of health records. Additionally, using social security number eliminates the need for patients to remember several identifiers by providing a single identifier for all kind of records. Such identifiers are also used for purposes out of healthcare, therefore, link the patient records with other records such as financial records. Such linkage endangers patient privacy in secondary uses of health information. For instance, disclosed medical records can be identified by third parties to whom the

records are disclosed using social security number. Identifiers such as social security number fail to satisfy identity protection.

In secondary uses of health records, such as research, the health records are de-identified to protect patient privacy. Records are de-identified by removing personally identifiable information (refer to 2.6.1). As mentioned before, patients may have several records in different healthcare organizations. De-identification and possession of several scattered records, lead to duplication of a particular patient information in research. Such hidden duplication reduces the accuracy of research. Additionally, In many cases, disclosed information may need to be re-identified (refer to 2.6.2). For instance, record owners should be re-identified and informed about any rare diseases found during research. Therefore, unique health identifiers are necessary in secondary uses of health records besides the primary uses.

2.4.1: ASTM criteria for evaluating proposed identifiers

Several identifiers has been proposed for unique health identifier. The American Society for Testing and Materials (ASTM) has defined 30 criteria for evaluating different candidates for a Universally Unique Health Identifier (UHID). Four basic functions of an identifier are supported by these criteria [29]:

- Positive identification of patients when clinical care is rendered.
- Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic health care files.
- Provision of a mechanism to support data security for the protection of privileged clinical information (does not attempt to address all safety concerns).
- Use of technology for patient records handling to keep health care operating costs at a minimum.

The 30 criteria of ASTM for evaluating proposals for a Unique Heatlh Identifier are [30]:

- Accessible (available when required).
- Assignable (assign when needed by trusted authority after properly

authenticated request).

- Atomic (single data item--no subelements having meaning).
- Concise (as short as possible).
- Content-free (no dependence on possibly changing or unknown information).
- Controllable (only trusted authorities have access to linkages between encrypted and non-encrypted identifiers).
- Cost-effective (maximum functionality with minimum investment to create and maintain).
- Deployable (implementable using a variety of technologies).
- Disidentifiable (possible to create a number of encrypted identifiers with same properties).
- Focused (created and maintained solely for supporting health care--form, usage, and policies not influenced by other activities).
- Governed (has entity responsible for overseeing system--determines policies, manages trusted authorities, and ensures proper and effective support for health care).
- Identifiable (possible to identify the person with such properties as name, birth date, sex, etc, by associating these with the identifier).
- Incremental (capable of being phased in).
- Linkable (can link health records together in both automated and manual systems).
- Longevity (designed to function for foreseeable future with no known limitations).
- Mappable (able to create bidirectional linkages between new and existing identifiers during incremental implementation of a new identifier).
- Mergeable (can merge duplicate identifiers to apply to the same individual).

- Networked (supported by a network that makes services available universally).
- Permanent (never to be reassigned, even after a holder's death).
- Public (meant to be an open data item--person can reveal it).
- Repository-based (secure, permanent repository exists to support functions).
- Retroactive (can assign identifiers to all existing individuals when system is implemented).
- Secure (can encrypt and decrypt securely).
- Splittable (able to assign new identifier to one or both people if the same identifier is assigned to two people).
- Standard (compatible if possible with existing or emerging standards).
- Unambiguous (minimizes risk of misinterpretation such as confusing number zero with letter O).
- Unique (identifies one and only one individual).
- Universal (able to support every living person for the foreseeable future).
- Usable (processable by both manual and automated means).
- Verifiable (can determine validity without additional information).

2.4.2: Options for Unique Health Identifiers

Several options have been proposed for Unique Health Identifier. These identifiers are divided into three main categories [30]:

1- Unique identifiers based on social security number:

- Social security number: using unenhanced form of the social security number.
- Proposal of The Computer-based Patient Record Institute (CPRI): based on the social security number with the addition

of check digits.

- Using an alternative identifier similar to the social security number.
- The Computed Healthcare Identifier (CHID): a new identifier would be computed from the social security number.

2- Unique identifiers not based on the social security number

- The ASTM sample identifier.
- Biometric identifiers.
- Personal immutable properties.
- Identifiers based on civil registration system.

3- Proposals That Do Not Require a Universal, Unique Identifier

- Master patient index: Use of a legacy system directories containing patient information and cross referencing directories to records in other sites.
- Identification Systems Based on Existing Medical Record Numbers with a Practitioner Prefix.

2.5: Primary uses and access control

Primary uses refer to all type of uses or disclosures of health information in order to provide treatment and health services to the patient. “Use” means the employment, application, utilization, examination, or analysis of protected information within a care provider that maintains information, whereas, “Disclosure” means the release, transfer, provision of access to, or divulging in any other manner of protected information outside the care provider holding the information [9].

Primary uses and disclosures are initiated and carried out by authorized users in care providers through access control mechanisms. Access control refers to “Limiting access to information system resources only to authorized users, programs, processes, or other systems.” [31] Access control has two main components:

- Authentication: ”Security measure designed to establish the validity of

a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information." [31]

- Authorization: "The granting of access rights to a user to a user, program, or process." [32]

Access control is not a complete solution to protect information unless it is coupled with auditing [33]. Auditing is "Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures." [31]

Authorized users, after successful authentication, gain access to the patient information. However, maintaining access to whole parts of health records to all authorized individuals are unnecessary. The minimum sub-set of health information required to carry out an individuals task or duty, which is called need-to-know information, should be specified for each role or individual.

2.6: Secondary uses, de-identification and re-identification

Secondary uses of health information refers to all uses or disclosures of the information for purposes other than treatment to health services, such as [9]:

- When required by law.
- For public health activities.
- For research and epidemiological purposes.
- About victims of abuse, neglect, or domestic violence.
- For health oversight activities.
- For judicial and administrative proceedings.
- For law enforcement purposes.
- About decedents.
- For donation of or organs, eyes, or tissues.

- To avert a serious threat to health or safety.
- For specialized government functions.
- For certain marketing purposes.

2.6.1: De-identification

In order to protect patient privacy, disclosed information should not identify record owners. De-identification is the process of removing or altering data in a health record that could be used to identify the record owner [34]. Removing identifiable information is not adequate to protect patient privacy. Using other databases, such as marketing and credit information, and using sophisticated and readily available tools, de-identified patient records could be linked with other databases [35]. As a result, altering parts of health records are necessary in order to adequately de-identify health records. For example, dates of hospital visits and discharges could be removed in order to prevent identification of patients with unique hospital visit patterns.

2.6.2: Re-Identification

"Re-identification is the discovery, or determination, of the identity of the individuals who are the subjects of a study through data linkage techniques." [36] Re-identification can only be done by care providers mentioned in the privacy policy. To re-identify records, each record should be labeled with a unique identifier. Such identifier should not identify record owner [37] by containing any personal identifiable information or publicly known unique identifiers. There should be a mechanism to label each de-identified record and to re-identify it if required. Care providers should not disclose the mechanism for re-identification [9]. Example or re-identification is when cases of a rare disease are found in a research study. To preserve the patient safety, the record owners whom believe to have such disease should be informed about their health condition. Re-identification could done by the record keeping care provider and the patients could be informed accordingly.

CHAPTER 3

STRUCTURING AND AUTOMATING THE PATIENT PRIVACY POLICY

3.1: Overview of existing policies

Most healthcare organizations have policies in order to protect patient privacy and EHR confidentiality while using and disclosing the health information. Such policies are represented in natural language and mainly consist of general guidelines. Some of the general requirements of privacy policies for healthcare are are [38]:

- Implementing procedures to protect health information.
- Establishing procedures to respond to privacy related complaints and inquiries.
- Training users.
- Informing public about the organization's polices and procedures.
- Privacy risk assessment and mitigation.
- Assigning a privacy officer to facilitate compliance with applicable data protection legislation and the following privacy requirements.
- Agreements with third parties about the legitimate uses and disclosures of health information.
- identifying purposes for use and disclosure.
- Limiting the collection of information to what fulfills the purpose of information gathering.
- obtaining patient consent.

- logging access, modification, and disclosure activities.

Some of the specifications of existing privacy policies are as follows:

- Existing policies are represented in natural language. This can lead to ambiguities and different interpretations.
- There is no agreed upon standard for structuring policies.
- Since HCOs use different polices represented in diverse languages and probably different propriety standards, there is no way to accurately affirm the privacy protection in shared care.
- Policies mainly contain general guidelines. There is no guarantee that the individuals affecting by the policy conform to its contents. As a result, there is an inconsistency between privacy policy and actual practices [39].
- Existing policies mainly cover the routine medical practices. Controversial medical practices are still dependent on case-to-case judgments [4].
- Revision and changing the policies are difficult and error prone.
- HCOs adopting new privacy polices undergo time consuming and costly organizational re-engineerings. As a result, HCOs become less desirable to change the polices in use.
- Policies often need revisions and changes according to the latest legislations on patient privacy. Some of these legislations require major changes in privacy policies, such as the elimination of consent requirement of the HIPAA rule [40].
- Hidden conflicts and errors in policies are difficult to locate and resolve.

3.2: Definitions and Reasons of structuring and automating the patient privacy policy

So far we have discussed some of the most important specifications of existing policies in their traditional form. These specifications make traditional policies unable to fulfill the privacy requirements of the electronic healthcare. "Having extensive privacy policies in an enterprise does not directly ensure privacy protection if there are no effective means of consistent policy enforcement across multiple applications and across enterprise boundaries." [41] The most important lacking features on existing policies are structuring and enforcement through automation.

Structuring means "the operation of imposing an order or organization on a set of information." [42] Structuring the policy makes it scalable and easier to review and change. To structure the privacy policies, various languages can be used, such as XML, P3P, EPAL, and XACML (refer to 3.3). Using such languages provides a standard way to represent the policy. This standardization facilitates interfacing the policies between different HCOs, hence, leads to privacy protection in shared care. On the other hand, structured policies are easier to check for errors and conflicts.

Automating the privacy policy means relying on computer systems to enforce the policy in an organization. Automation ensures the effective conformation to the policy. Furthermore, it reduces the human labor for policy management , thus, reducing human errors. Automating facilitates the immediate reflection of latest policy changes to daily practices.

Privacy policy covers various healthcare processes and regulates the actions of a wide variety of individuals involved in care providing process. Electronic healthcare has introduced new aspects in healthcare and has changed the existing processes considerably. What follows is different aspects of electronic healthcare affecting by privacy policy and the resulting benefits of structuring and automating the policy.

3.2.1: Electronic health records (EHRs)

The most significant aspect of electronic healthcare is EHR. "The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this

information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports." [43]

The benefits and unique roles of EHR are [44, 45]:

- Immediate and universal access to the patient record.
- Easier and quicker navigation through the patient record.
- No lost charts.
- Standardization of care among providers within the organization.
- Clinical data that is formatted to be easy to read and analyze.
- Reduction of paperwork, documentation errors, filing activities.
- Coding efficiency and efficacy.
- Alerts for medication errors, drug interactions, patient allergies.
- Ability to electronically transmit information to other providers.
- Availability of clinical data for use in quality, risk, utilization, ROI analyses.
- Basis for decision support.
- Serves as the legal document describing the healthcare services provided.
- A major resource for healthcare practitioner education.
- Represents a provider-based view of that patient's health history.

As mentioned in the EHR benefits, unlike paper based records, EHR is an omni-present document which can be accessed simultaneously from different locations. EHR is mainly used for primary uses of health information. For such primary uses, access control mechanisms should be in place in order to regulate the access level of authorized users and denying the access of unauthorized users (refer to 2.5). For secondary uses, such as research, the EHR should be de-identified by removing all personally identifiable information (refer to 2.6.1).

Managing the privacy policy and protection of EHR's confidentiality becomes complex and ineffective with unstructured and paper based privacy policies, mainly

because of the:

- Complexity of EHR: EHR is a comprehensive document which contains the lifelong health status of an individual. Covering all parts of EHR, make the unstructured policies complex and error prone.
- Accessibility of information: EHR is accessible to different individuals. In electronic healthcare different parties from medical and non-medical professions may need to have access to the EHR. Those accessing the EHR may belong to different roles with different access rights. The roles in healthcare are apt to intersect, for instance a physician may be a member of "specialist" role and "hospital staff" at the same time. The diversity of authorized people with different and over-lapping access rights makes the unstructured policies complex and ineffective in protecting confidentiality.
- Context based access rights: Access rights to EHR may change according to the context of care providing. For instance, a nurse may need to have access to EHR while the patient is in the hospital. After discharge, the access of the nurse may need to be restricted. This type of context based access control is difficult to manage with the static nature of traditional policies.
- Restriction of access to vital information: Policies may contain unnecessary restriction on health information. This leads to the lack of availability of vital information such as allergies, medications in use, and chronic diseases. Unstructured policies may contain such hidden restrictions. Structured policies on the other hand can be analyzed programatically to locate any hidden deficiencies.

3.2.2: Decision making

In modern electronic based HCOs, different individuals from diverse professional backgrounds work collaboratively in decision making processes regarding the patient health. On the other hand, the participation of patients are encouraged through what is called "shared decision making." [46] This diversity of

individuals affecting the outcome of decision making, necessitates a new approach to manage policies.

Another issue in decision making is the medical practice for which the decision is to be made. Existing policies mainly cover the routine medical practices. However, the realm of healthcare is replete with unpredicted situations which are not addressed by existing policies. On the other hand, there are some controversial issues in healthcare. There is not an agreed upon decision for such issues because physicians, patients and other decision makers hold different religious and moral values. Examples of such controversial practices are:

- abortion.
- blood transfusion among Jehovah witness believers [47].
- organ transplantation of brain dead patients [48].
- Assisted suicide [49].

As Winkler argues, an organization wide policy which covers all individuals in HCO and deals with both standard and morally controversial medical practices ensures autonomy, quality, fairness, and efficiency of decision making processes [4]. Traditional policies which mainly covers the routine practices is not suitable with the collaborative decision making model of electronic healthcare. Structured policies on the other hand can be updated as soon as new consensus on unpredicted and controversial issues have been reached. By automating the policy, the latest changes reflect to the daily practices accordingly. On the other hand, different policies could be defined according to patients' consent for controversial issues. Additionally policies could be enriched by sophisticated decision support softwares to assist decision makers in unpredicted situations.

3.2.3: Shared care

In addition to the collaborative efforts of various individuals in a single HCO, several HCOs may cooperate in providing healthcare by sharing EHR or parts thereof. Considering the mobility of population and cost reduction requirement of HCOs, cross organizational access to medical information would certainly be beneficial, for instance by avoiding unnecessary examinations [50]. In such a cross-organizational information sharing, the referring and referred HCOs may encompass

flawless privacy policies, however, problems may arise due to the differing levels or standards of privacy protection applied in HCOs. Some of the privacy policy problems relating to shared care is as follows:

- Privacy violation: A less restrictive privacy policy in the referred HCO may lead to the privacy violations. For example, the referred HCO may grant access to a role or individual whose access is denied in the referring HCO.
- Unavailability of vital information: A more restrictive policy in the referred HCO may deny the access of authorized and legitimate users to vital information, such as allergies, HIV status, and chronic diseases. Unavailability of such vital information lead to diverse consequences due to the wrong decisions made.
- Patient safety: Both problems discussed so far, namely privacy violation and unavailability of vital information, endangers patient safety. The former may maintain the patients' access to the parts that should be kept hidden from them for their own safety. The later problem could have life threating consequences by denying access to vital information.
- Differing standards and languages: Different HCOs may use different standards to represent and manage the policies. for example, the referred HCO may grant access rights to roles, yet the referring HCO may use individual identities instead. HCOs located in different countries may use different languages to represent policies.
- Lack of interface: There should be an interfacing mechanism to check and bridge the policies of HCOs involving in shared care. Such an interface is necessary to assure the policy protection level of different HCOs. An example of such privacy protection assurance is the “Safe harbor” which acts as a bridge to ensure the adequacy of privacy protection of non-European Union nations as defined by European Directive on Data Protection.

All these problems are intensified by the fact that unstructured policies are used in HCOs. Checking and interfacing unstructured policies is a time consuming and

error prone activity. However, structured policies could be checked programatically to find any unnecessary granting or denying of access. Using standard structuring languages facilitates the interfacing and bridging of privacy policies between HCOs.

3.2.4: New standards and legislations

Healthcare practices are influenced by various national or universal standards and legislations. Such standards and legislations are apt to rapid upgrades and changes. An example of an aggressive change is the elimination of "informed consent" requirement of HIPAA rule [51]. In this constant influx of re-framings, new versions of standards or rules are released prior to any implementation or organizational adaptation. Moreover, a standardized policy based on universally accepted standards is difficult to apply due to different national laws framing the management of policies in different countries. Hence, any policy should be flexible and dynamic enough to conform to necessary changes in a timely manner. Additionally, Automating the policy provides the HCOs with an ongoing compliance with changing laws and standards. A structured and automated policy provides the necessary flexibility and timely conformity to changing standards and rules.

3.2.5: Conflict resolution and ethical checks

Traditional healthcare based on a simple physician-patient relationship model, has been changed dramatically by the new innovations of electronic healthcare. So far we have discussed some of these changes such as complex division of labor, electronic health records and shared care. As a result of such changes, the healthcare processes have become more complex compared to the traditional medical practices. Privacy policy covers different aspects oh healthcare. Consequently policies covering the new aspects of electronic healthcare are more comprehensive, hence, more complex than traditional policies. Comprehensiveness and resulted complexity will cause the booming of hidden conflicts and worse, errors in the policy.

To counter the hidden errors resulted by constant changes, regular poliy assessment in necessary. Charl van der Walt [52] proposes some questions to asses the security policy. The same questions, with minor modifications, could be used to

assess the privacy policy as well:

- Does the policy have a clearly defined scope? Is it clear to which system and which people the policy is applicable?
- Does the policy clearly define responsibilities?
- Is the policy enforceable? Can it be applied in a concrete manner so that the compliance is measurable?
- Is the policy having its desired effects?
- Is the policy universally known and understood within the organization? Is the policy well distributed, is there an awareness of the policy and is its content understood?
- Does the policy comply with law and with duties to third parties? Is the organization fulfilling its statutory obligations?

Policy assessment and finding errors and conflicts are inefficient with unstructured policies. However, structured policies can be analyzed programatically to find any hidden conflict and error. Such analysis helps HCOs to ensure the validations and verification of their polices.

3.2.6: Accountability and auditing

Automated and machine controlled policies have a potential to act as a paternalistic controlling entity by moving from guidance to imposing force on parties in electronic healthcare. Similarly, Winkler states that [4], “policies guide individual action and thereby constitute the collective action of the organization.” On the other hand, highly restrictive policies endanger patient safety. For instance, policy may deny the access to staff on duty in an emergency case where the authorized users may not be available on time. Thus, non-flexible policy enforcement can bring undesirable consequences by compromising autonomy of decision makers and by endangering patient safety.

Therefore, protecting privacy from one hand should be in balance with patient safety and decision makers' autonomy on the other hand. To reach such a balance, mechanisms are needed to override restrictions posed by the policy in specific cases.

However, such overrides should be audited comprehensively. Auditing enables later analysis of such overrides and tracing back the actions to accountable individuals.

It should be noted that auditing here refers to logging overrides of restrictions posed by the policy not logging all actions done on EHR. A computerized privacy policy can be enriched by sophisticated auditing analysis tools to provide the accountability service.

3.2.7: Informed consent

Depending on the givens of a certain privacy policy, informed consent can provide wide variety of information to the patients. It can also affect the decision making processes if such processes are conditioned by consent and patient agreements. New approaches to represent and implement consent policies are needed to respond to the changes posed by electronic healthcare. For instance, a mechanism to provide patients with customizable privacy policies and to ensure patient safety are necessary since such customizations can cause restriction of access to vital information. It is an advantage of a structured policy that it enables a thorough analysis to expose any undesirable restrictions or privacy leaks.

3.3: XACML for structuring the policy

"XACML is an OASIS standard that describes both a policy language and an access control decision request/response language (both encoded in XML)." [53] The objectives of XACML are:

- " To Create a portable and standard way of describing access control entities and their attributes.
- To Provide a mechanism that offers much finer granular access control than simply denying or granting access -- that is, a mechanism that can enforce some before and after actions along with "permit" or "deny" permission." [54]

3.3.1: Benefits of XACML

According to the Sun's implementation guide [53] The benefits of XAMCL are:

- It is standard. Using the same standards language facilitates interoperability.
- It is generic. A single policy can be used by many different kinds of application. Additionally, policy management becomes easier using a standard common language.
- It is distributed. Rather than having to manage a single monolithic policy, different people or groups can manage separate sub-policies as appropriate, and XACML knows how to correctly combine the results from these different policies into one decision.
- It is powerful. It supports a wide variety of data types, functions, and rules about combining the results of different policies. In addition to this, there are already standards groups working on extensions and profiles that will hook XACML into other standards like SAML and LDAP, which will increase the number of ways that XACML can be used.

3.3.2: XACML components:

XACML is composed of several components. The following is an overview of concepts and components of XACML [53, 54]:

- Policy: contains a single access control policy. Access control involves the subject, resource, action, and environment, all governed by Rules. A Policy contains one or more Rules.
- Rule: Specifies the subject issued the access, resource to be accessed, action of the request, and optional environmental properties of the request.
- Subject: Specifies the requester of access. It specifies an individual, a role, or an application.
- Resource: The entity for which an access request has been issued. For instance, it represents a server, a file, or a part of EHR.

- Action: Specifies the type of access to the resource, such as read, write, delete and so on.
- Environment: environment properties of the access, such as date or time range. Environment is an optional feature.
- Attribute: Are the specifications of subject, resource, action, and environment.
- PolicySet: specifies a set of Policies or PolicySets. A PoliySet contains one or more Policies.
- Request: Is a access request containing the attributes of at least one subject, resource, action, and environment.
- Response: Is a result of an request evaluation. A response contains one or more Results, Status (e.g. the reason for denial), and optional obligations to be done before granting or denying access. the results could be one of the following [55]:
    - Permit
    - Permit with Obligations
    - Deny
    - Not Applicable (the PDP cannot locate a policy whose target matches the required resource)
    - Indeterminate (an error occurred or some required value was missing)
- Obligation: Provides finer-level access rights than simple permit and deny access types. After evaluating the request, PEP is responsible to enforce both evaluation result and operations specified in obligation.
- Target: Not all the PolicySets, Policies, or Rules undergo evaluation process when a request arrives. Target is a simplified condition on subject, resource and action to specify the PolicySets, Policies, and Rules that should be evaluated for a request.

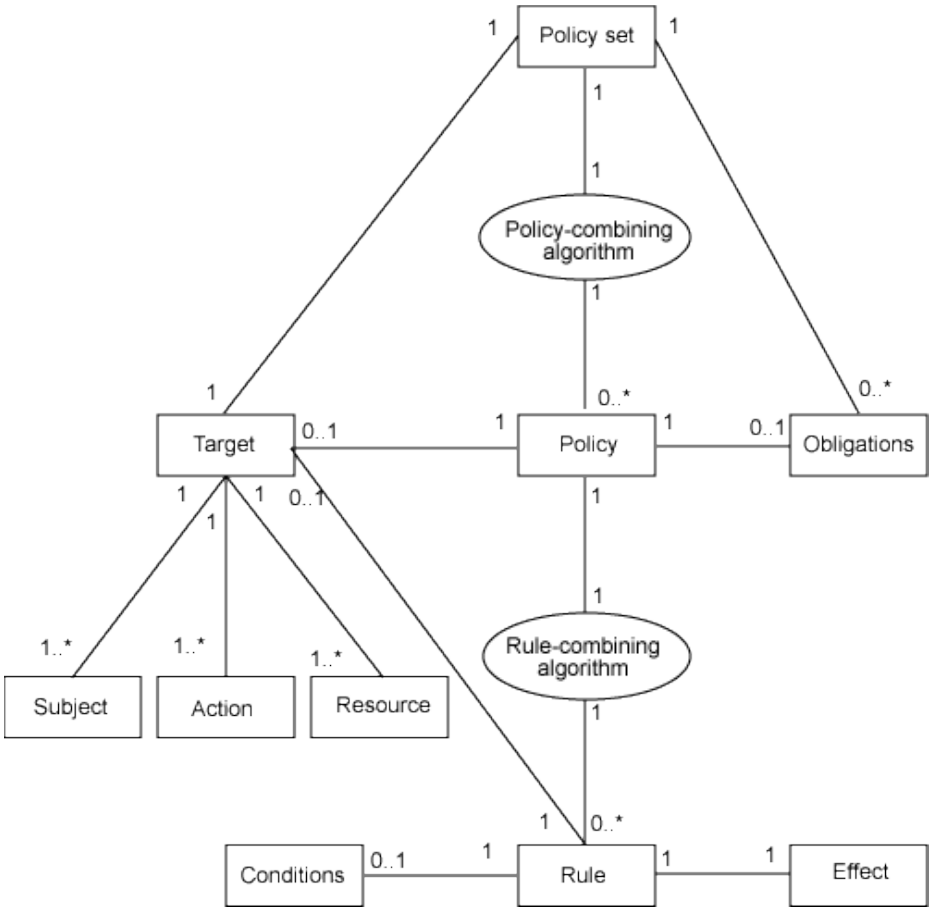

Figure 3-1: XACML policy language model [54]

- Policy-combining algorithm and Rule-Combining algorithm: When a request arrives several PolicySets, Policies, and Rules may be evaluated with probably conflicting results. Policy-combining algorithms and rule-combining algorithms are used to combine such conflicting results into one final decision.
- Policy Enforcement Point (PEP): is responsible of creating requests and interpreting responses. It typically interacts in an application-specific manner with its environment. Is is also responsible of fulfilling the obligations.
- Policy Decision Point (PDP): is responsible of evaluating the request and generating the response.
- Policy Access Point (PAP): is responsible of writing PolisySets and Policies and make them available to PDP.

- Policy Information Point (PIP): is responsible of retrieving attribute values related to subjects, resources, and actions.

3.3.3: XACML sequence of actions

The following is the sequence of actions from issuing a request to the returning of a result, as depicted in figure 3-2 [54]

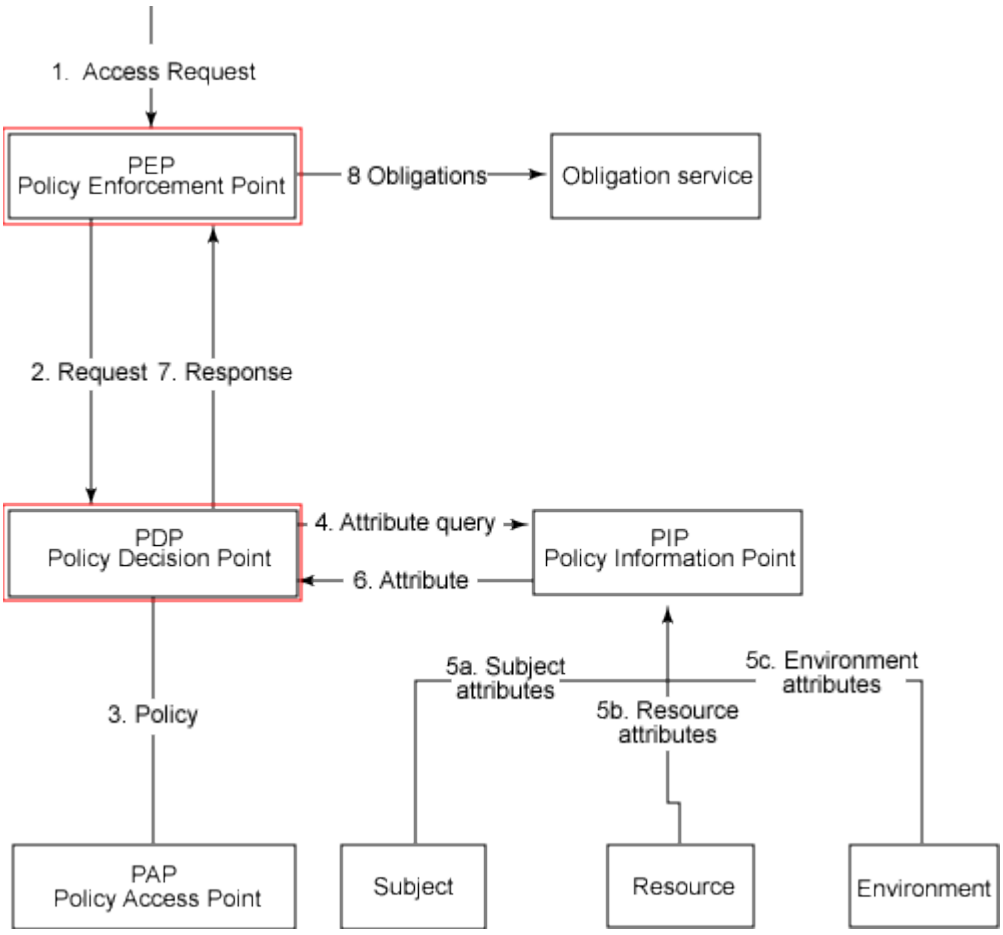

Figure 3-2: XACML main components

1- User issues an access request. The application sends the request via its API to PEP.

2- The PEP makes a standard request and sends it to the PDP.

3- The applicable policies for evaluation are returned from PIP to PDP.

4- A query containing the subject, resource, and action attributes of the

request is formed and sent to the PIP.

5- Attributes required for request evaluation is retrieved. The attributes relate to subjects, resources, and environments.

6- PIP sends retirieved attributed to PDP.

7- PDP evaluates the request against Policies and PolicySets found. The decision is sent to PEP.

8- PEP applies the obligations over the decisions sent by PDP to derive the final decision.

3.3.4: XACML codes

The following XML code is a sample XACML request in which a subject (user ID = “sethUserID”) has requested a “view” type of access to a resource labeled as “confidential”.

```
<Request>
<Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject">
<Attribute AttributeId="username" DataType=
"http://www.w3.org/2001/XMLSchema#string"
Issuer="admin@users.example.com">
<AttributeValue>sethUserId</AttributeValue>  </Attribute>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType= "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
<AttributeValue>seth@users.example.com</AttributeValue>  </Attribute>
</Subject>
<Resource>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType= "http://www.w3.org/2001/XMLSchema#anyURI">
<AttributeValue>confidential</AttributeValue>  </Attribute>
</Resource>
<Action>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType= "http://www.w3.org/2001/XMLSchema#string">
```

```
<AttributeValue>view</AttributeValue> </Attribute>
</Action>
</Request>
```

The following XML code is a sample XACML policy. The target of the policy restricts the application of this policy to the requests whose subject is “GP”. the resource and action parts of the Targer is any, which means the only factor to choose this policy is the subject part of the request. There first rule of this policy applies to “view” action on “Personal_Identifiable” resources. The effect of this rule is “permit”. In other words, the first rule of the policy permits the “view” access right to “Personal_Identifiable” resources. The final rule of the policy is “Deny”. In case that no rule is found for a request, the final rule specifies the final decision.

```
<Policy PolicyId="policy_id" RuleCombiningAlgId=
"urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-
overrides">
<Description>
This policy applies to Role GP  accessing Personal-Identifiable classification
level objects. Final fall-through rule that returns Deny.
</Description>
<Target>
<Subjects>
<Subject>
<SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
<AttributeValue DataType=
"http://www.w3.org/2001/XMLSchema#string">GP</AttributeValue>
<SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
</SubjectMatch>
</Subject>
</Subjects>

<Resources>
<AnyResource/>
</Resources>
```

<Actions>
<AnyAction/>
</Actions>
</Target>
<Rule RuleId="Personal-Identifiable" **Effect="Permit"**>
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType=
"http://www.w3.org/2001/XMLSchema#anyURI">**Personal-Identifiable**</AttributeValue>
<ResourceAttributeDesignator AttributeId=
"urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType=
"http://www.w3.org/2001/XMLSchema#string">**view**</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType=
"http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="FinalRule" **Effect="Deny"**/>
</Policy>

The following XML code is a sample XACML response. It specifies the decision ("Permit" in this example), and the status of the decision.

```
<Response>
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

3.3.5: comparison with other languages

In this study, the candidate languages for structuring privacy policies were XML, P3P, EPAL and XACML. The following is a brief overview of these languages.

- XML: "XML is a markup language for documents containing structured information. Structured information contains both content and some indication of what role that content plays.A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents." [56]

  XML is the base language for P3P, EPAL, and XACML. Although it is possible to structure policies using pure XML, it leads to non-standard policies. Such structured policy may satisfy all the requirements of a single healthcare organization, however, it fails to interact with policies of other organization. The design of structured policies based on pure XML is difficult because all features, such as role based access control, should be studied and implemented by the organization.

- P3P: "The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that

can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit." [57]

The main purpose of P3P policies is to automate the policy protection activities of web sites. "P3P can only express privacy promises related to specific information collection instances on an organization's website. Two main deficiencies of P3P according to [58] are:

- P3P cannot express the general privacy policies of the organization as a whole.
- P3P is not enforceable and it is subject to different interpretations [59] (as cited in [58]). As a result, P3P statements are inherently ambiguous.

- EPAL: "The Enterprise Privacy Authorization Language (EPAL) is a formal language to specify fine-grained enterprise privacy policies. It concentrates on the core privacy authorization while abstracting from all deployment details such as data model or user-authentication." [60] EPAL is a language created by IBM. The following are the goals of EPAL [61]:
    - Provide the ability to encode an enterprise's privacy-related data-handling policies and practices.
    - A language that can be imported and enforced by a privacy-enforcement systems.

The following are the applications of EPAL [61]:

- Rule Creation by a Privacy Administrator.
- Interoperability of Privacy Software Products.
- Privacy Enforcement.
- A Privacy Audit.

The Differences of EPAL and P3P are [62]:

- *Categories*: P3P has a pre-defined list of data categories. EPAL allows for an enterprise to define its own list of data categories and these may be hierarchical.
- *Data-Users*: P3P has a pre-defined list of data users. EPAL allows for an enterprise to define its own list of data users and these may be hierarchical.
- *Purposes*: P3P has a pre-defined list of purposes. EPAL allows for an enterprise to define its own list of purposes and these may be hierarchical.
- *Actions*: P3P only defines the action "use". EPAL allows for a definable list of actions.
- *Conditions*: P3P does not define a condition language. EPAL uses the XACML condition language.
- *Obligations*: P3P only defines the obligation "retention". EPAL allows for a definable list of obligations.
- *Choices*: P3P only allows for simple opt-in/opt-out choices. EPAL allows for a more generalized set of choices.

"While EPAL and XACML are very similar in structure and concept, the differences between the languages are significant, and greatly affect their usability and their ability to meet the requirements of an enterprise privacy policy language." [63] Table 3-1 shows the differences between EPAL and XACML.

Table 3-1: Differences between EPAL and XACML

Feature	***Difference between EPAL and XACML***
Decision request	EPAL supports a subset of XACML
Rule	EPAL supports a subset of XACML
Applicability of rules	EPAL supports a subset of XACML
Condition	Equivalent
Nested policies	EPAL does not support
Result conflicts	EPAL supports a subset of XACML

Table 3-1 (continued)

Feature	***Difference between EPAL and XACML***
Policy references	EPAL does not support
Vocabulary	XACML supports a subset of EPAL
Attribute mapping	EPAL supports a subset of XACML
Attribute retrieval	Equivalent
XML attribute values	EPAL does not support
Hierarchical roles	EPAL does not support
Hierarchical categories	XACML does not support
Hierarchical resources/XML document resources	EPAL supports a subset of XACML
Subjects with multiple attributes	EPAL supports a subset of XACML
Multiple subjects	EPAL does not support
Purpose attribute	EPAL supports a subset of XACML
Error handling	EPAL does not support
Revision number	Equivalent
Data types	EPAL supports a subset of XACML
Functions	EPAL supports a subset of XACML
Obligations	EPAL supports a subset of XACML
Multiple responses	EPAL does not support
Status as a standard	XACML is an OASIS standard EPAL is not a standard

CHAPTER 4

STRUCTURED PATIENT PRIVACY POLICY (S3P): DESCRIPTION AND ARCHITECTURE

4.1: Background

The main aim of privacy policy is to regulate the actions of individuals involved in care providing. Privacy policy management and enforcement becomes more complex with a shift to electronic healthcare. The reasons for such complexity are the diversity of parties involved in care providing and cross organizational information sharing (refer to 3.2). "Having extensive privacy policies in an enterprise does not directly ensure privacy protection if there are no effective means of consistent policy enforcement across multiple applications and across enterprise boundaries." [22] "Often privacy policies are hardcoded into enterprise applications and services or managed with very vertical, ad-hoc solutions, in specific contexts. This approach is not adaptive to changes and does not scale. The enforcement of privacy rights, permissions and obligations on confidential and personal data requires the mapping of these concepts into rules, constraints and access control, the meaning of which must be unambiguous so that it can be deployed and enforced by software solutions. This still requires following best practices and good behaviors. However, automating aspects of the enforcement of privacy policies can really help enterprises to improve their practice and simplify the overall management." [64]

It is obvious that non-enforceable privacy policies, regardless of their content and comprehensiveness, are not adequate to protect privacy. In order to model a structured and enforceable privacy policy, we have designed the Structured Patient

Privacy Policy (S3P).

4.2: The definition and the process of S3P prototype development

S3P or Structured Patient Privacy Policy, is a prototype application which models a structured and enforceable automatic privacy policy. It is a JAVA based application designed with an incremental software process model. It formalizes a privacy policy based on eXtexsible Access Control Markup Language (XACML). Additionally, it simulates access control for primary uses and disclosure options for secondary uses of health records. The access control is based on an extended Role Based Access Control (RBAC) model.

As mentioned before, S3P is a prototype application. The Figure 4.1 depicts the process of S3P prototype development [65]:

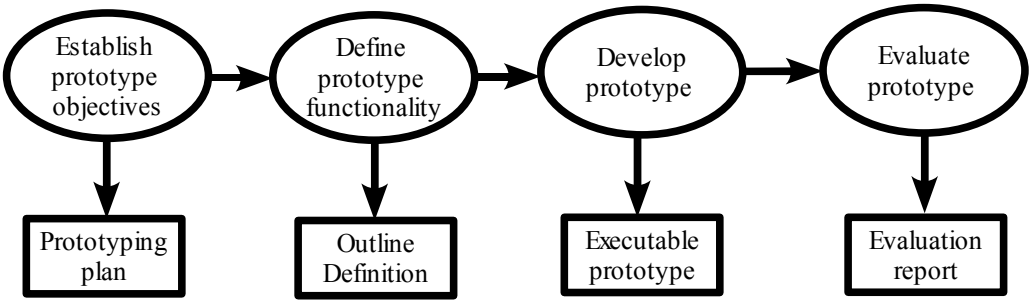

Figure 4.1: The process of prototype development

This study covers only the first three steps of prototype development. For detailed information about the first increment of the development refer to 4.5. For Information about the future increments refer to 6.3.

4.3 The objectives of S3P:

The objectives of S3P are:

- To provide a framework for structured and enforceable privacy policy.
- To provide a prototype application in order to elicit the actual

requirements of enforcing the electronic privacy policies.

- To provide a simulation of automated patient privacy policy.
- To simulate a structured policy based on a standardized language to assist further studies on interfacing policies between different HCOs.
- To provide a means for experts from different professional backgrounds to assess the affect of structured and enforceable privacy policies on healthcare processes.
- To provide a means to highlight the new aspects of privacy protection in electronic healthcare.
- To highlight the technical, procedural, and ethical problems of privacy protection in electronic healthcare to assist the experts to collaboratively find the most appropriate solutions.

4.3.1: S3P High level user requirements:

In this section a high level user requirements of S3P is presented. Since the S3P is a prototype application, its development has begun without gathering the actual requirements of potential users. The target users of S3P are experts from different professional background. As a result, the requirements have been prepared in a general way so that it covers the possible requirements of all potential users.

- To model a fictitious EHR.
- To partition and classify the EHR to reflect the differing sensitivity levels of its contents.
- To provide access control for primary uses based in Role Based Access Control (RBAC).
- To provide options for secondary uses.
- To provide informed consent with opt-in and opt-out options.
- To provide auditing for accountability.
- To represent the privacy policy in a structured and standard way.

4.4: S3P prototype functionality and System requirements

In this section the system requirements of S3P framework are presented. The focus in developing process was on the functional requirements of the S3P. Such requirements states the services and the functionality of the system. Table 4.1 shows the seven main services on S3P.

Table 4.1: Services of S3P framework

Service	*Details*
EHR management	-Defining and maintaining access to a fictitious EHR
Classification and Labeling	- Classes of confidentiality - Labeling the EHR with confidentiality classes
User Management	- Defining roles - Assigning users to roles - Unique Health Identifier - Authentication
Access Control	- Authorization - Privileges - Emergency & Granted
Disclosure Options	- De-Identification - Re-Identification
Informed consent	Notice of Privacy practices
Audit policy	- Accountability

4.4.1: EHR management

This service involves with defining and managing the access to EHR for primary or secondary uses. The EHR in S3P is based on a fictitious record driven from LifeSensor sample health record [66]. The outline of the contents of an EHR in S3P is as follows:

- Profile
  - Personal
  - Employment
  - Insurance

- Present and past illnesses
    - Problems
    - Medical visits
    - Symptoms
    - Diagnoses
    - Tests
    - Procedures
    - Hospitalization
- Medications
    - Present medications
    - Medication schedule
    - Past medications
- Emergency data
    - Profile
    - Contacts
    - Emergency contact
    - Healthcare contact
    - Blood data
        - Blood type
        - Blood transfusion
    - Heath risks
        - Personal risks
        - Family risks
    - Diagnosis
    - Procedures
    - Implants

- Allergies
- Immunization
- Present medications

- Laboratory reports
  - Current tests
  - Past tests

4.4.2: Classification and Labeling

The main aim of the privacy policy is to protect the confidentiality of the information during any kind of access to EHR. However, various portions of EHR require different levels of protection. For instance, HIV status or mental health notes require a higher level of protection comparing to an X-ray image result. This heterogeneity of confidentiality levels of EHR portions necessitates a mechanism to classify different segments of EHR.

Classification is the categorization of objects according to their qualities or extrinsic information attributed to them to help in their management [67]. The classification in S3P ensures the need-to-know principle which will be covered in Access control service (refer to 4.4.4).

Classes of confidentiality:

The first step in classification service is to define confidentiality classes. The following confidentiality classes have been defined in S3P. However, S3P is not limited to the following classes. New classes can be added to the system and existing classes can be edited or deleted.

- Not identified yet: For newly defined EHR portions.
- Personal identifiable-level 1: For personally identifiable information such as name, last name, and mother name.
- Personal identifiable-level 2: For information that is not automatically identify a person but can be used to spot the record owner, such as gender, age, eye color.

- Demographical: Living area, Contact information, address, telephone,...
- Public: Information that can be disclosed without endangering patient privacy. For example, the general condition and the room number of a patient in a hospital.
- Private: Information that is unnecessary to be disclosed for non-treatment purposes. Disclosure of such information should be done according to the consent and after de-identification of the records.
- Hidden-from-patient: Some portions of EHR may need to be hidden from patient for their own safety. Examples of such information is HIV status at the initial stages of diagnoses and the psychiatry notes.
- Confidential: undesirable disclosure of this level endangers the privacy. Examples of confidential portions are mental health treatments, and suicide history.
- Confidential-Hidden: Highly confidential information that need to be hidden from patient.

The classification approach used in S3P is not hierarchical. It means that those who have access to the "Confidential" portions of the EHR does not necessarily have access to less confidential portions such as "Public". For more details about the access to confidentiality classes refer to (4.4.4).

Labeling the EHR with confidentiality classes:

After defining the confidentiality classes, the EHR portions should be labeled with those classes. The process of labeling in S3P is done through masking each portion of EHR with one and only one confidentiality class. The labeling in S3P is not a static process. The confidentiality level of portions of EHR may change due to an initial wrong labeling. Another reason for such changes is that the confidentiality of some portions of EHR may change over time. For instance, the HIV status may be hidden from patient only at initial phases of diagnosis. Therefore, Labeling in S3P is a dynamic process in which label if each potion can be changed easily.

4.4.3: User management

This service involves with unique health identifier, authentication, creating users, creating roles, and role assignment. Figure 4.2 depicts the use case of user management service.

Unique Health Identifier:

As mentioned in 2.4, Unique health identifier (UHI) is necessary for duplication prevention, research accuracy, and efficient administration. UHI in S3P is for uniquely identify each EHR and only used to identify patients. Since there is only one hypothetical EHR in S3P, this service does not contain any specific mechanism for UHI management. However, the module is designed so that the future increments to the software can easily be added and implemented.

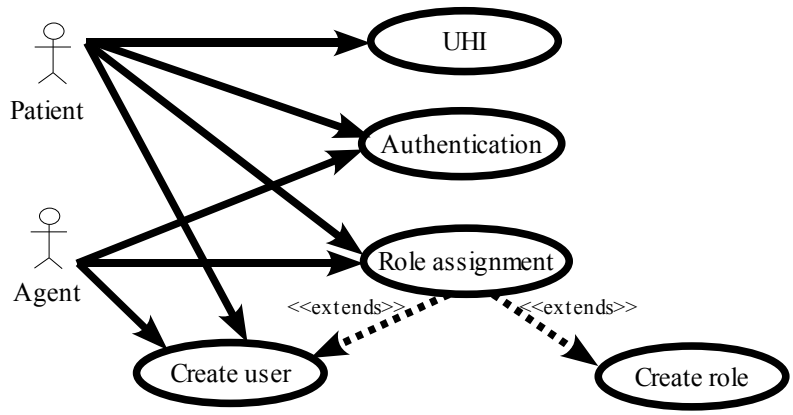

Figure 4.2: Use case diagram of the user management service

Authentication:

The authentication in S3P is based on user name and password. The patients and healthcare agents need to be authenticated before accessing the EHR for any purpose.

Creating user:

New users can be added to S3P using this service. Users can be patients or healthcare agents. In this service each user is assigned with a unique username and a password.

Creating roles and Role assignment:

Each agent in a care provider needs to have access to a sub-set of EHR in order to accomplish his or her task. However, there are many individuals in a care provider and assigning access rights to individuals is extremely time consuming and error prone. The access control rights in S3P is granted based on Role Based Access Control (RBAC). "A role can represent a collection of users, and a user can be a member of multiple roles." [68] Users or agents are groups into roles according to their profession, duty, or position. In the pure RBAC model, access rights are assigned to roles not to individual, hence, reduce the burden of administrator in access right assignment.

S3P provides a means to create new roles and assign users or agents to roles. The following are the features S3P provide related to role assignment, some of which are extension to RBAC:

- **Hierarchical roles:** S3P provides a means to define hierarchical roles. In hierarchy of roles, a role can be defined as a child role to an existing role. The child role inherits all the rights of parent role. For example, in S3P there is a role that represents "Specialists" which is the parent role of the "Surgeon" role. In this case, the "Surgeon" inherits all the rights of "Specialist" role. However, it is possible to change the rights of the child role in S3P by increasing or decreasing the inherited roles. As a result, there is no guarantee that the access rights of the child role is necessarily is less than the rights of its parent role.

- **Multiple roles:** A user or agent can be the member of multiple roles. For example a specialist may be the member of "Oncologist" and "Hospital staff" at the same time. In this case, the agent holds the access rights of both roles. There could be differences in the access rights of multiple roles. For example, the "Confidential" class may be accessible to one role and non-accessible to the other. In S3P, the least restrictive right or the most restrictive right of multiple roles can be chosen.

- **Individual access granting:** RBAC allows access right granting only to roles. In S3P, it is possible to assign access rights to individuals

whose rights might be different from their other roles. In such a case, the least restrictive right or the most restrictive right of roles and individual can be chosen.

- **Context based access control:** RBAC does not contain context based access control. The access rights of roles are the same regardless of time, place or context of access. However, in S3P, the access control can be context based. The time and place of access can be influence the access decision result.
- **Labeling:** Rather than labeling information, RBAC associates each roles with a specific set of operations that the individual acting in that role may perform [69]. S3P, however, incorporating the labeling for classifying the information with the RBAC model.

4.4.4: Access control

Access control service provides the actual access right assignment to roles or individuals. Figure 4.3 depicts all possible services of access control.

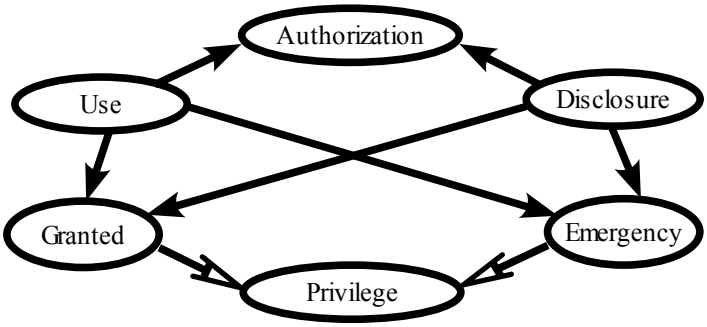

Figure 4.3: Services of Access Control

Two main services of Access control are:

- Authorization: Refers to providing access to authorized users as predefined by policy makers or administrator according to the privacy policy.
- Privilege: Refers to providing access to unauthorized agents or

temporarily heightening the access rights of authorized agents in specific cases. The following are two reasons for Privilege access type.

- Granted: Access right is assigned to unauthorized agent by authorized agents for consultation or shared care. The access rights of the referred agent is equal or less than the rights of the referring agent.
- Emergency: If and when the restrictions posed by policy prevents care providing in emergency cases, the access rights of authorized agents can be increased. Furthermore, unauthorized agents can be granted predefined temporary access rights.

Both Authorization and Granted access types include two types of uses of EHR information:

- Uses: Refers to all uses of health information for treatment and care giving purposes.
- Disclosure: Refers to all uses of health information for non-treatment purposes such as research and education.

Access right assignment for primary purposes in S3P is done by defining the following items :

- Subjects: The legitimate uses should be defined for each role or individual which are the subjects of access right service. The default access right for all roles is denial of access.
- Resource: The accessible resource (confidentiality classes) for each subject should be defined.
- Action: The legitimate actions done by subjects on resources should be defined. Examples of actions of primary uses of EHR are add, delete, view, and ament.
- Context: The time, place, and context of access.

Figure 4.4 depicts the “authorization” service with the details of some “actions”.

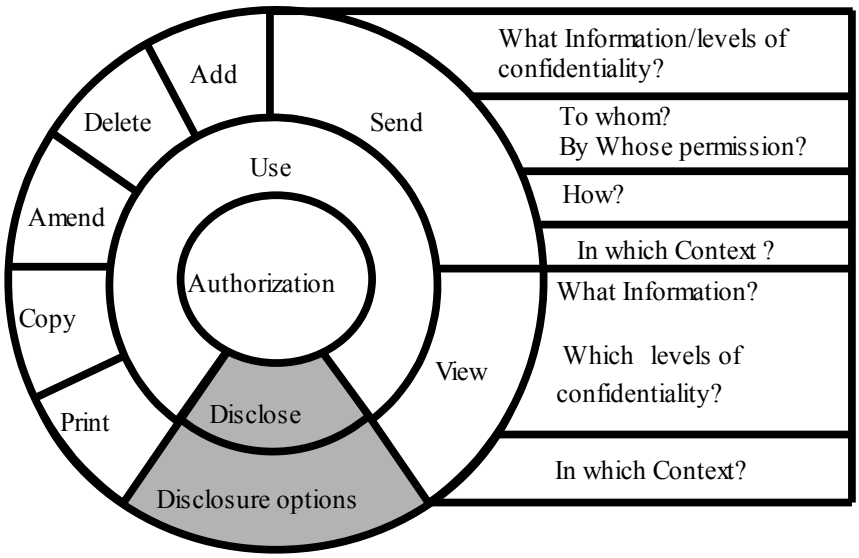

Figure 4.4: Authorization service

4.4.5: Disclosure Options

Disclosure service specifies the potions of EHR, in terms of confidentiality classes, that should be removed in order to de-identify the records. The de-identification in S3P is done through removal of the confidentiality classes that the administrator specifies. The inclusion of any confidentiality class in de-identification process leads to the removal of all portions associated with that class. If only a sub-section of any confidentiality class needs to be de-identified a new confidentiality class should be defined and masked on that sub-section. Example of such sub-class category in S3P is the "Numerical personal identifiable".

The disclosed information should be specified in accordance with minimum necessary standard. Minimum necessary standard limits the disclosed information to an amount necessary to accomplish the secondary uses purposes [70].

In order to provide re-identification, any UHI that is not directly identify the patient and is not a public identifier can be used to identify disclosed information.

4.4.6: Informed consent

Informed consent in S3P is a document containing the uses and disclosures or EHR. For primary uses, it contains the the following

- The roles who have access to EHR.
- The confidentiality classes that are accessible to each role.
- The legitimate actions and context of the accesses.

For secondary uses, it clarifies the confidentiality classes that need to be de-identified along with the purpose of disclosure and receiving roles or individuals.

4.4.7: Audit policy

All actions done by agents on EHR, let it be use or disclose, should be audited. Auditing ensures accountability which hold the agents responsible of the actions they have done. It also provides non-repudiation which prevents the denial of involvement in any actions done on EHR.

4.4 S3P design and development:

In this section the design and development of the S3P is presented. The most important features of S3P design and development are:

- S3P is a prototype application.
- S3P is designed and developed with an incremental software process.
- It is based on the object oriented model.
- It is developed with JAVA language using Java Development Kit (JDK) version 1.5.0 [71].
- The structuring is done using OASIS XACML language. The Sun XACML implementation (version 1.2) is used [72].

The first version of S3P, which is the focus of this study, covers the primary authorization service based on RBAC, simple disclosure options based on hiding the specified confidentiality classes, non-hierarchical classification and labeling, hierarchical roles, and multiple roles. The UHI, statistical sound disclosure

techniques, opt-in/opt-out based consents, and context based access controls are increments considered for future version.

S3P contains several packages as depicted in Figure 4.5.

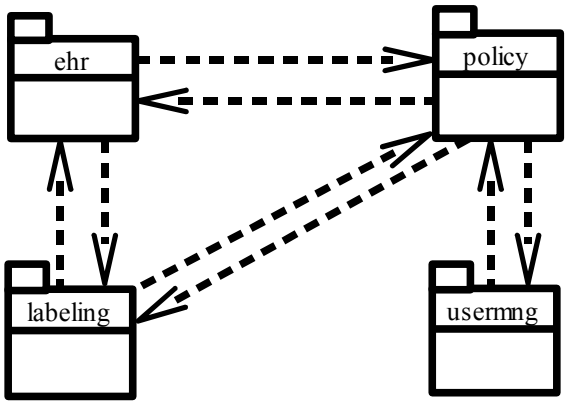

Figure 4.5: S3P packages

4.4.1: "ehr" Package

The ehr package contains classes to define, manage, and represent the EHR. There is only one EHR in the first version of S3P. The following are the classes in ehr package:

- SuperRecord: Is the class of all sub-section of EHR. It can contain several instances of itself. It also contains a parameter holding the confidentiality label.
- SuperField: Is the class of simple EHR entries. Intances of this class does not contain any other SuperField or SuperRecord class instances. SuperField is inherited form SuperRecord class. Through polymorphism there are several types of SuperField instances such as string, integer, float, array, boolean, date, and hash table.
- EntityId: Is a class used in SuperField and SuperRecord instances to uniquely identify each object of the EHR. This class is not used in the first version of the S3P and is considered for next increments. The purpose of this class is to provide access control to SuperField or

SuperRecord instances directly. In the the first version, the access control is done through confidentiality labels. EntityId uses an string value as an identifier. The format of the string is like “00-00-0-0000”. The characters of this string represent the following information:

- 0,1 characters = record
- 3,4 characters = sub record
- 6 character = field type
- 8,9,10,11 characters = field ID

- SuperEhr: Is the class containing the whole EHR. It consists of several instances of SuperRecord class. The instances of SuperRecord class in SuperEhr are:
  - Profile: The personal information. It consist of 3 instances of SuperRecord which are Personal, Employment, Insurance.
  - Illnesses: The information about past and present illnesses. It consists of several instances of SuperRecord including Problems, MedicalVisits, Symptoms, Diagnosis, Tests, Procedures, and Hospitalization.
  - Medication: The informations about past and present medications. It consists of SuperRecord instances including PresentMedication, PastMedication, and MedicationSchedule.
  - Emergency: The emergency information of the patient. It consists of SuperRecord instances including Contacts, HealthRisks, BloodData, Implants, Allergies, and Immunization.
  - LabReports: Contains the laboratoty test resutls of the patient. It consists of SuperRecord instances including CurrentTests, PastTests.

Figure 4.6 depicts the class diagram of the classes in ehr package. It also shows the implementation of an interface by SuperRecord class. The “ToolkitInterface” interface contains the global parameters that all classes from all packages need to have access. It contains the followint parameters:

- User Vector: A vector containing the users.
- Role Vector: A vector containing the roles.
- ClassLabelMaker instance: The object containing the confidentiality labels.
- MakePdp instance : The object containing the PDP.

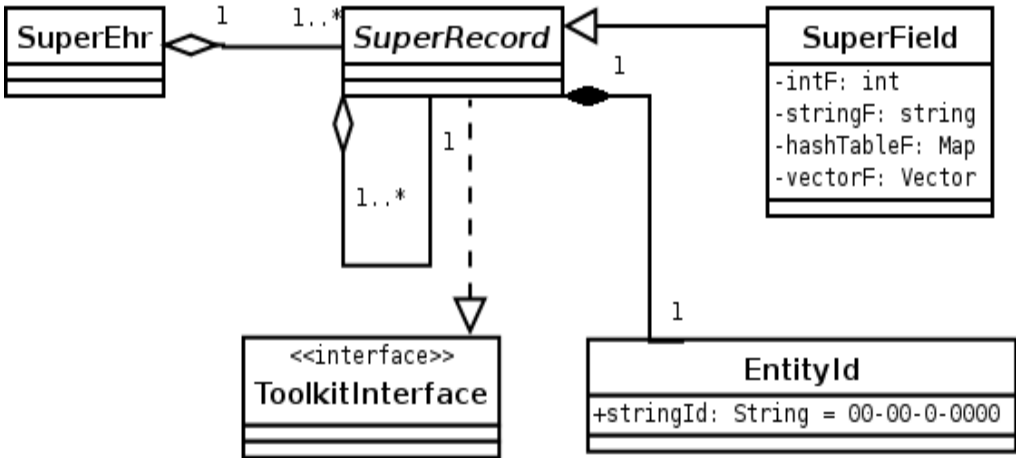

Figure 4.6: Class diagram of “ehr” package

Figure 4.7 shows a snap shot of EHR management panel that is accessible by the administrator of S3P. The figure shows the details for the personal part of the “Profile” sub-record of the EHR. The administrator can enter the Entity Id value as string. The confidentiality label can be specified from this panel as well.

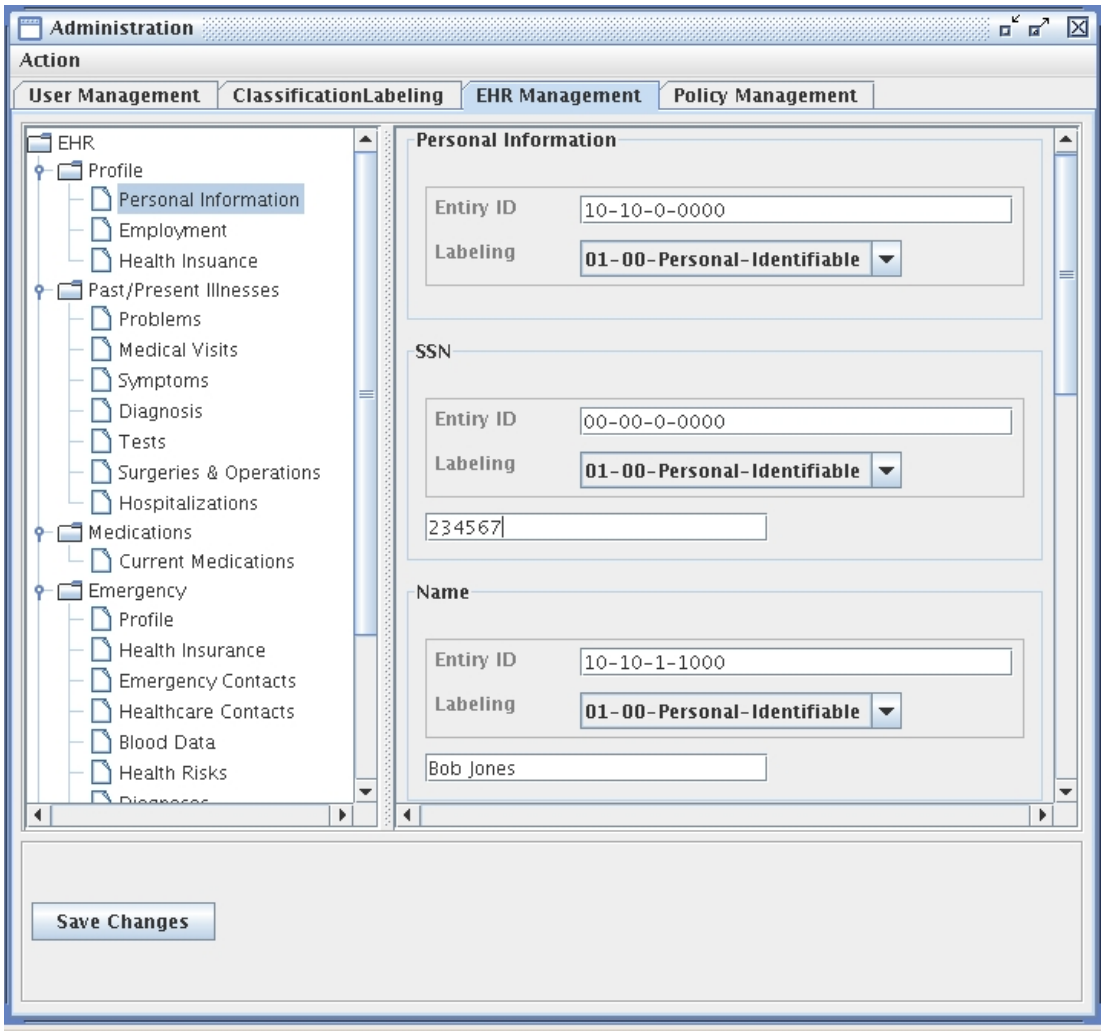

Figure 4.7: EHR management panel snap shot

As mentioned before, the type of the SuperField is specified using polymorphism by overloading the constructor. For a simplified code of SuperRecord refer to Appendix C.

4.4.2: “labeling” Package

The labeling package contains classes to define and manage the confidentiality classes and use them to label the EHR portions. This package consists of two classes:

- ClassLabel: Is a class representing a single confidentiality class. It contains the name of the class, the description of the class, and a unique identifier for each class. It also holds a vector of other

ClassLabel instances in order to make sub-classes of different types. For instance, “Personal Identifiable” class can have several sub-classes of “numeric”, “string”, and “multi-line string” types. The sub-class vector is considered to be used in the future versions of S3P. In the first version a new top level confidentiality class should be defined for different types of each class.

- ClassLabelMaker: Contains all defined ClassLabels. A static instance of this class is accessible to all classes implementing the “ToolkitInterface” interface.

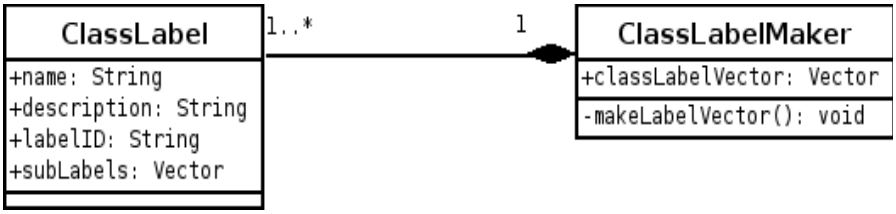

Figure 4.8: Class diagram of “labeling” package

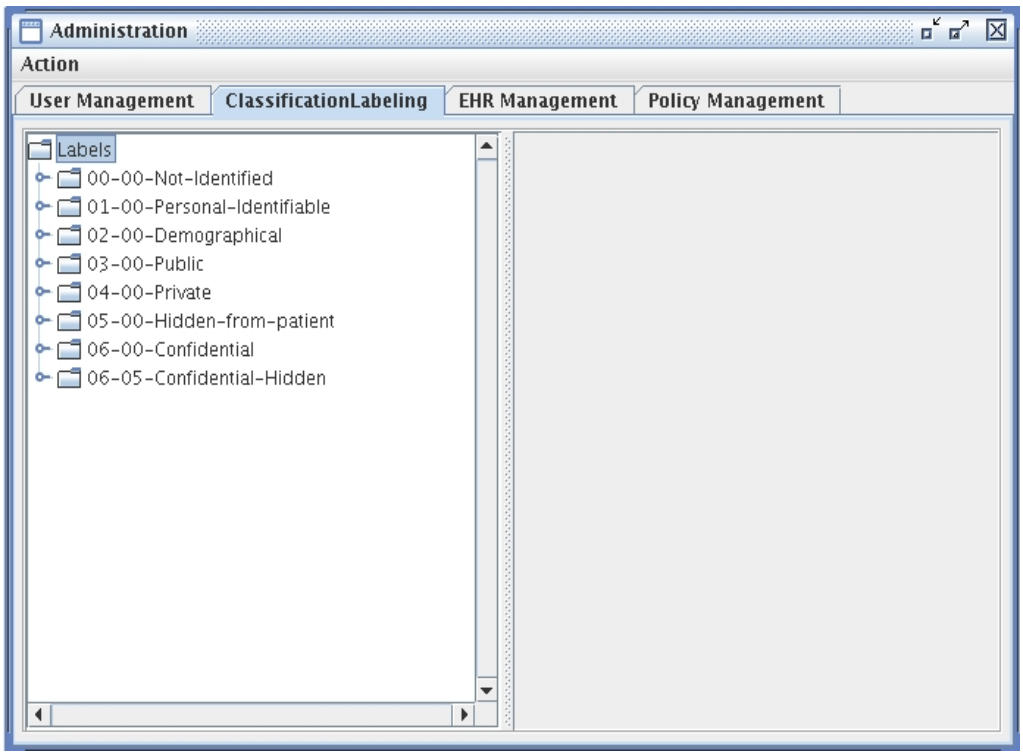

Figure 4.9: Classification management panel snap shot

Each SuperRecord contains a “labelId” string value which indicates the confidentiality class of that SuperRecord or SuperField. It is a simple 5 character string. The first two characters represent the main class, such as “personal identifiable”. The last two, which are separated from first two by using a dash, represent the type of the class, such as numerical or string. The code to find the full confidentiality class using the simple class label is represented in appendix C.

4.4.3: “usermng” Package

This package contains classes related to managing the users, , managing the roles, and assigning users to roles. The classes in this package are the basis for RBAC model. This package consists of the following classes:

- User: This class represents the agents of HCOs.
- UserCollection: This class contains instances of User class.
- Role: This class represents the roles in HCO. As mentioned in section 4.4.3, hierarchical roles are used in S3P. For this reason, each instances of this class has a parent role and a collection of children role. It also contains a vector holding the role members.
- RoleCollection: This class contains instances of Role class.

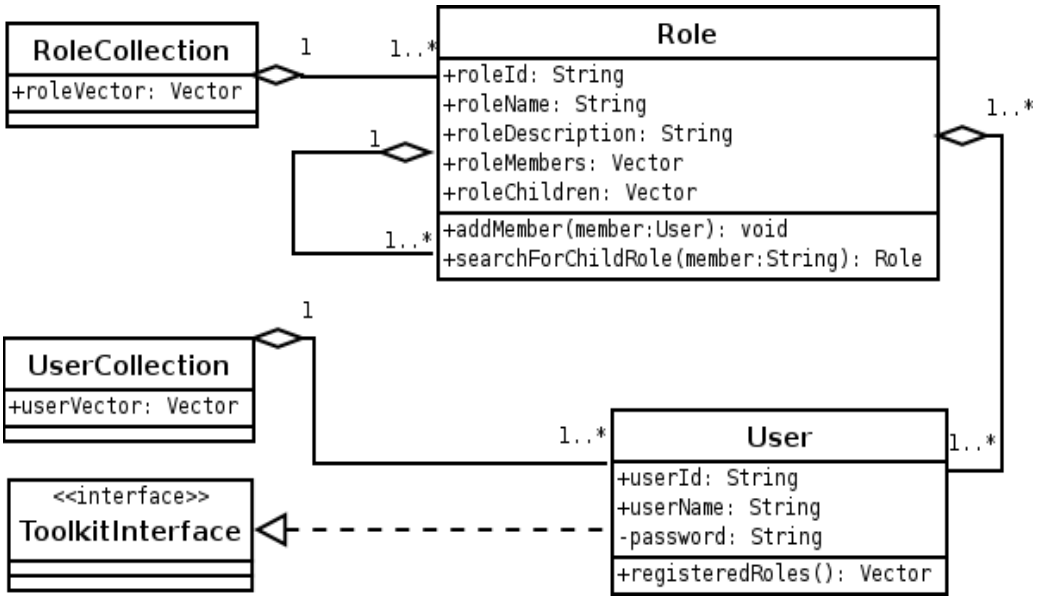

Figure 4.10: Class diagram of the “usermng” package

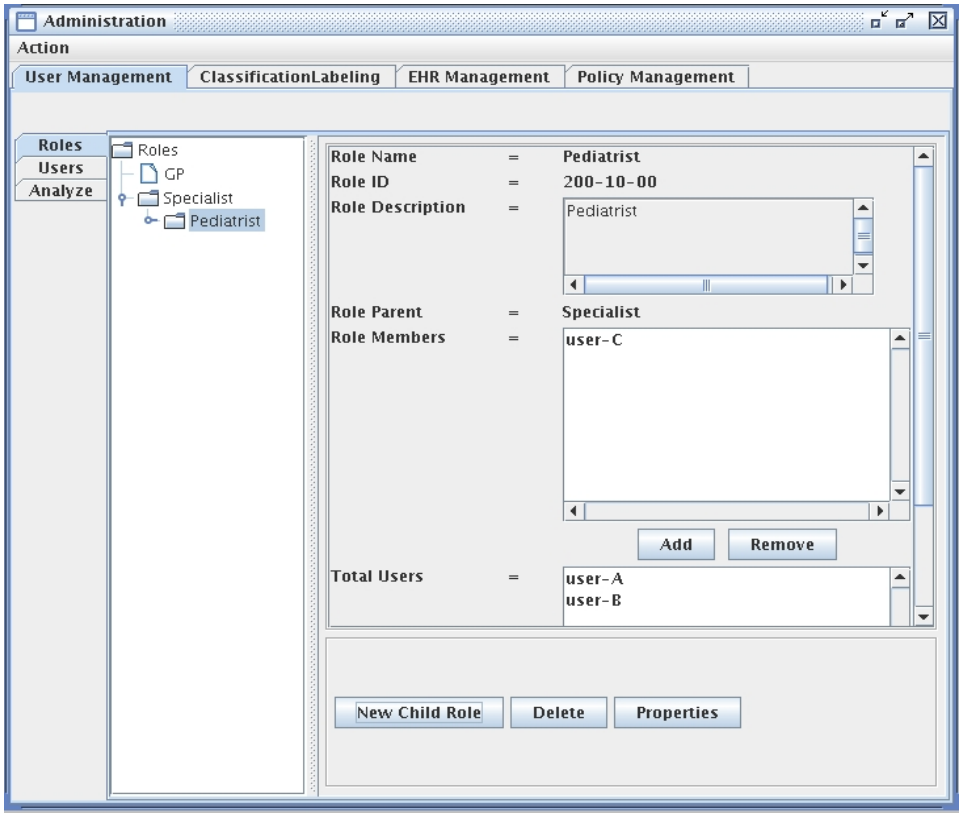

Figure 4.11: Role management panel snap shot

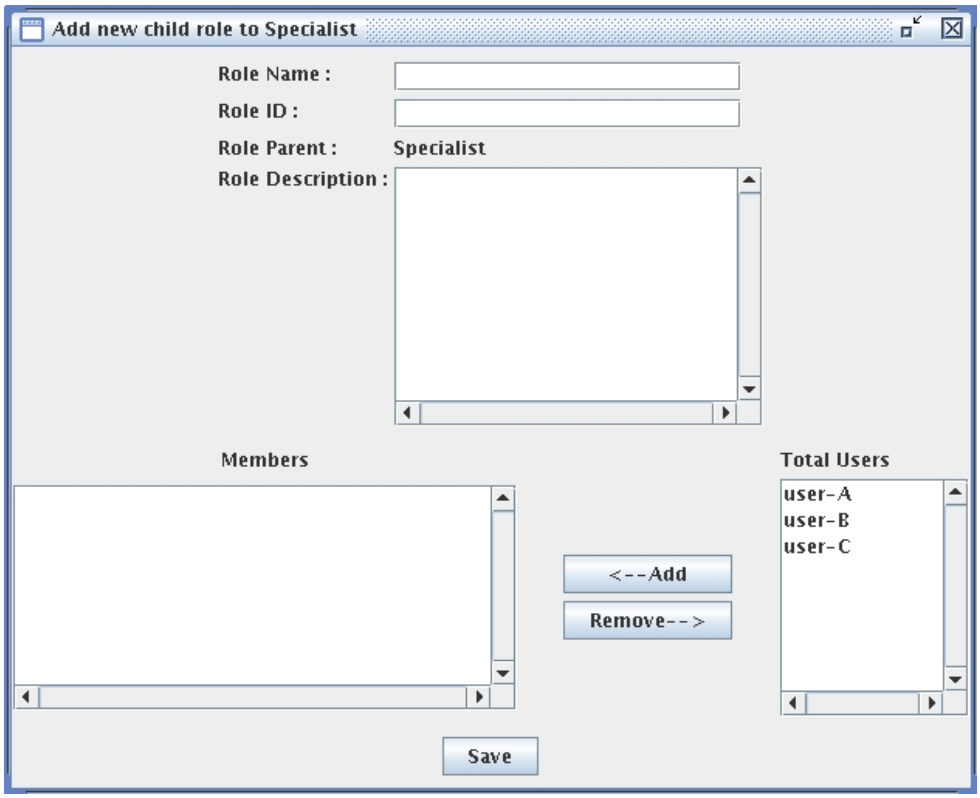

Figure 4.12: Snap shot of adding a new child role

4.4.4: “policy” Package

This classes of this package are responsible of defining and managing the XACML policy, checking the access request against the policy, providing the primary and secondary uses of EHR, and producing the informed consent.

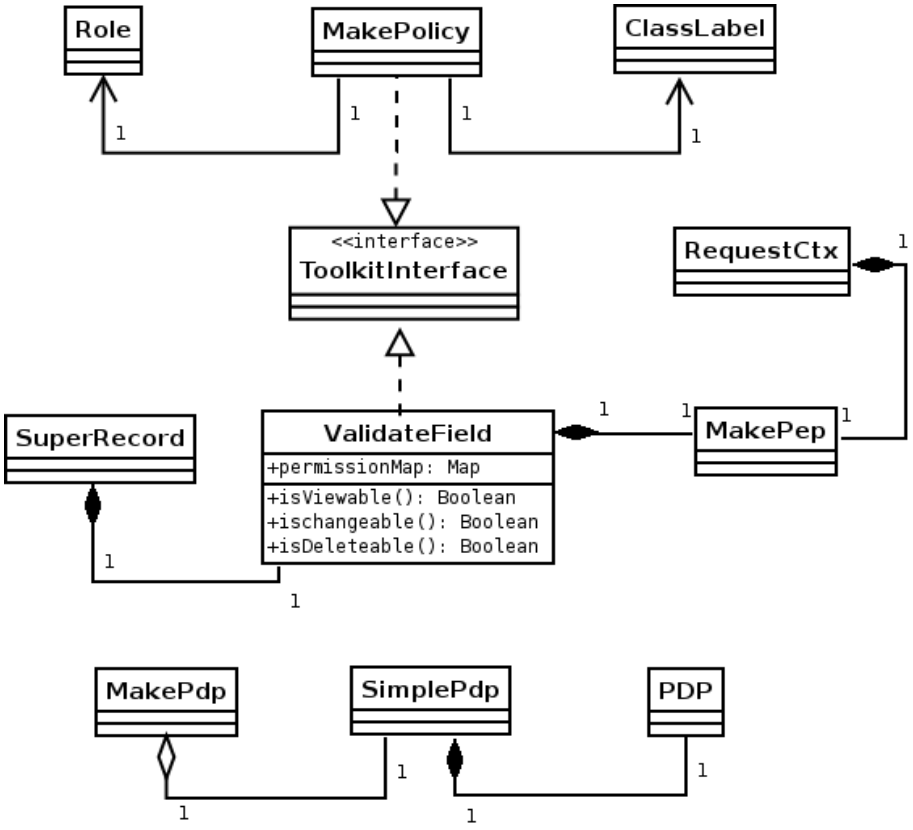

Figure 4.13: Class diagram of the “policy” package

The following is a list of the classes of this package:

- MakePolicy: This class is responsible of making XACML policies for all the combinations of roles and confidentiality classes. At first no policies exist for the roles. This is interpreted by the S3P as a deny of any kind of action. For a sample policy code refer to appendix C.

- MakePdp: This class initiates an object from SamplePdp class. MakePdp is accessible to all classes implementing the “ToolkitInterface” interface.

- SamplePdp: This class holds an instance of XACML PDP class (refer to 3.3.3). It also sends the policies to the PDP.

- MakePep: This class initiates a RequestCtx object from the XACML om.sun.xacml.ctx package. The request will be evaluated used by PDP.
- ValidateField: This class is initiated in every SuperRecord object. Upon the access request to the SuperRecord, this class makes a RequestCtx request and sends it to PDP for evaluation. It also holds the evaluation results.

Figure 4.14 depicts the access right assignment administrative panel. In this snap shot, the administrator is granting the access right to the "GP" role, to access the confidentiality class "Personal Identifiable". In this example, the permission to perform "view" and "change" actions has been set to "Permit". As a result of such a access assignment, all members of "GP" role can view and change the "Personal Identifiable" confidentiality classes.

Figure 4.15 depicts the sequence diagram of an access right evaluation. Each SuperRecord contains a ValidateField object. ValidateField makes an XACML Request using the role of the agent and the confidentiality label of the SuperRecord. It then sends an evaluation message to PDP, and receives back the result of the decision. It then turns the decision into boolean access rights for all predefined actions.

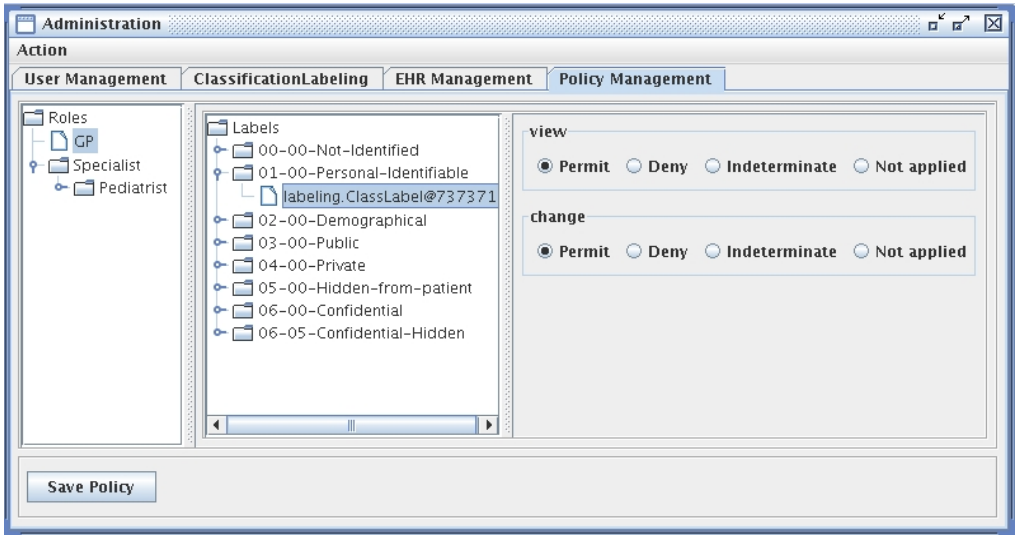

Figure 4.14: Snap shot of assigning access right by the administrator

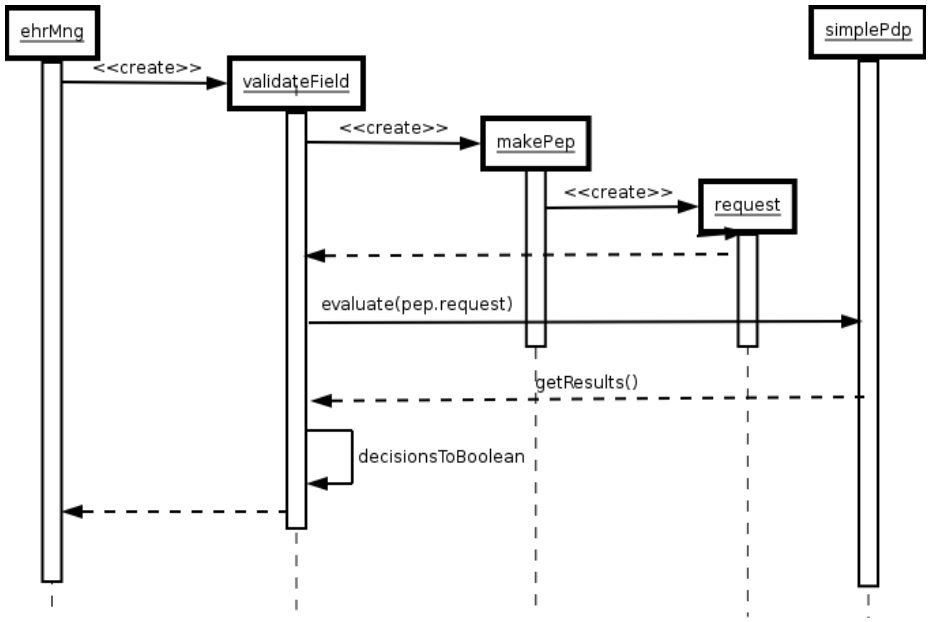

Figure 4.15: Sequence diagram of getting the access rights

4.4.5: Snap shots of an example

In this example, the “view” and “change” actions are tested on “Blood Data” confidentiality class. The example scenario is as follows:

- The blood data of the patient contains the blood type, RH factor, and HIV status, which is positive for this patient.
- The entire “Blood Data” portion, “Blood type”, and “RH type” are labeled as “Public” , whereas, the “HIV status” is labeled as “Confidential”. The labeling of “Blood Data” portion is shown in Figures 4.16 and 4.17.
- The roles to be used in this example are Oncologist, Nurse, MRI assistant, and insurer (Figure 4.18).
- The oncologists' access rights are as follows (Figure 4.19, 4.20):
    - Permission to view and change the “public” classes.
    - Permission to view and change the “confidential” classes.
- The nurses' access rights are as follows (Figure 4.21, 4.22):
    - Permission to view and change the “public” classes.

    - Permission to view but not to change the “confidential” classes.
- The MRI assistants' access rights are as follows (Figure 4.23, 4.24). The XACML policy of this rule can be found in appendix C.
    - Permission to view but not to change the “public” classes.
    - Denial of view or change the “confidential” classes.
- The insurers' access rights are as follows (Figure 4.25, 4.26)
    - Denial of view or change the “public” classes.
    - Denial of view or change the “confidential” classes.
- User-D logs in as “Oncologist” role as depicted in Figure 4.27.
- User-D can view and edit all the fields according to the access rights assigned. (Figure 4.28)
- User-E logs in as “Nurse”.
- User-E can view and edit the blood type and RH type fields, however, he or she cannot edit or change the HIV status field. The editable property of the HIV status combo box is disabled. (Figure 4.29)
- User-F logs in as “MRI assistant”.
- User-F can view the blood type and RH type fields, however, he or she can not edit or change them. The HIV status field is not accessible by User-F. (Figure 4.30)
- User-G logs in as “Insurer”.
- User-G can not view any fields of the “Blood Data” portion. The reason is “Blood Data” is labeled as “public” and the “Insurer” role does not have a permision to view the “public” classes. (Figure 4.31)

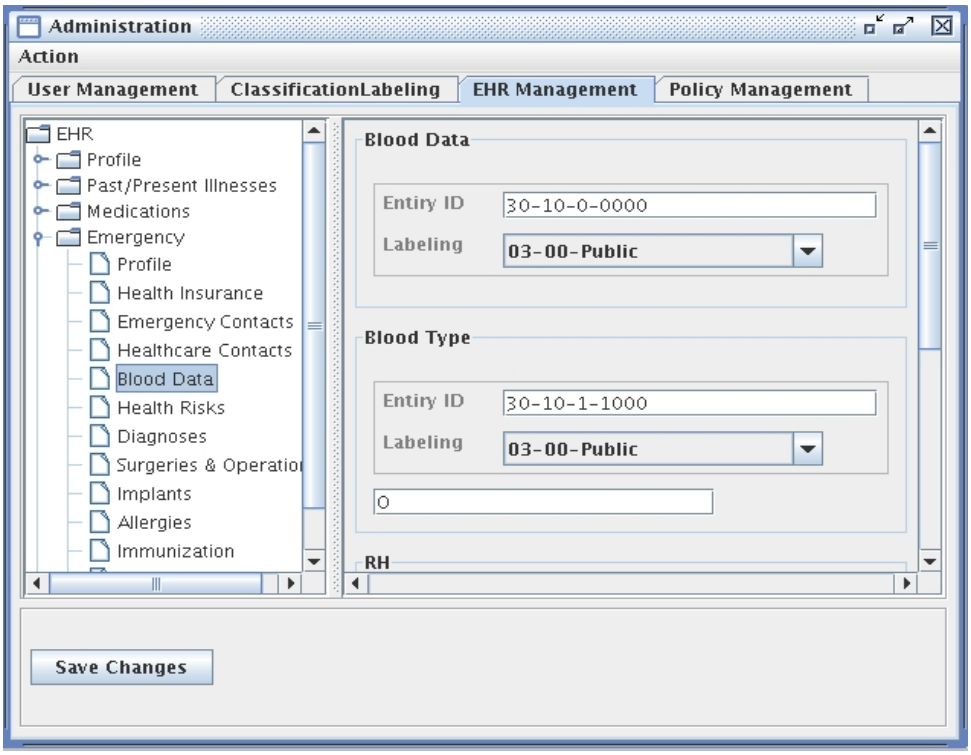

Figure 4.16: Labeling the "Blood Data" portion

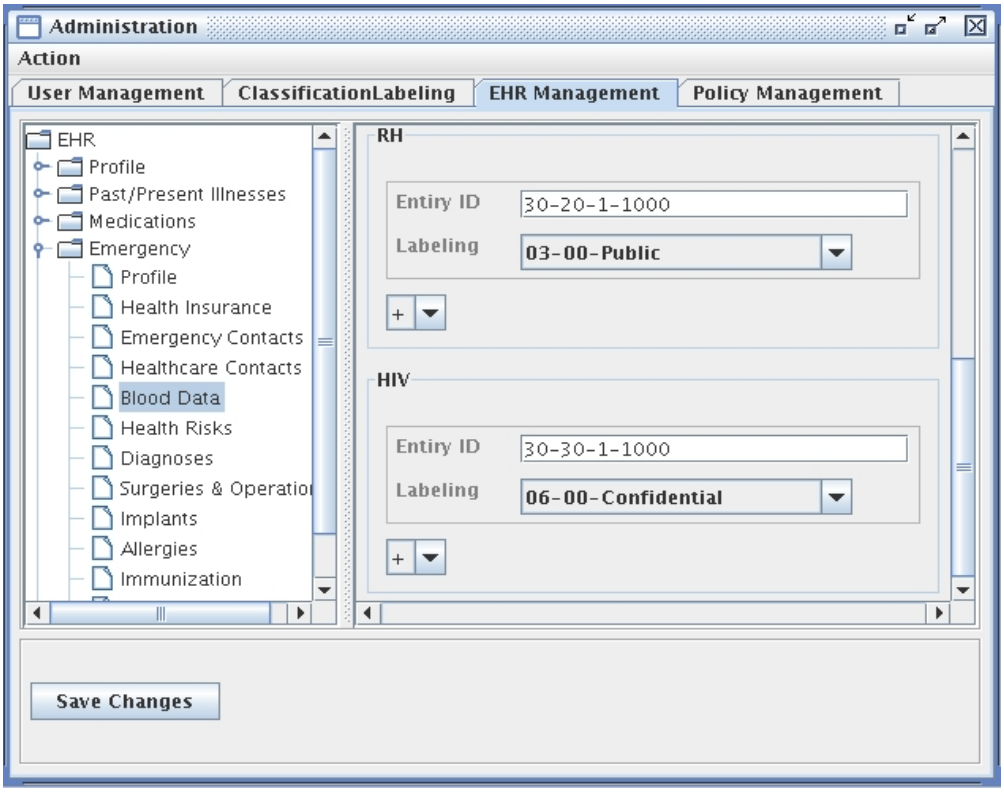

Figure 4.17: Labeling the "Blood Data" fields

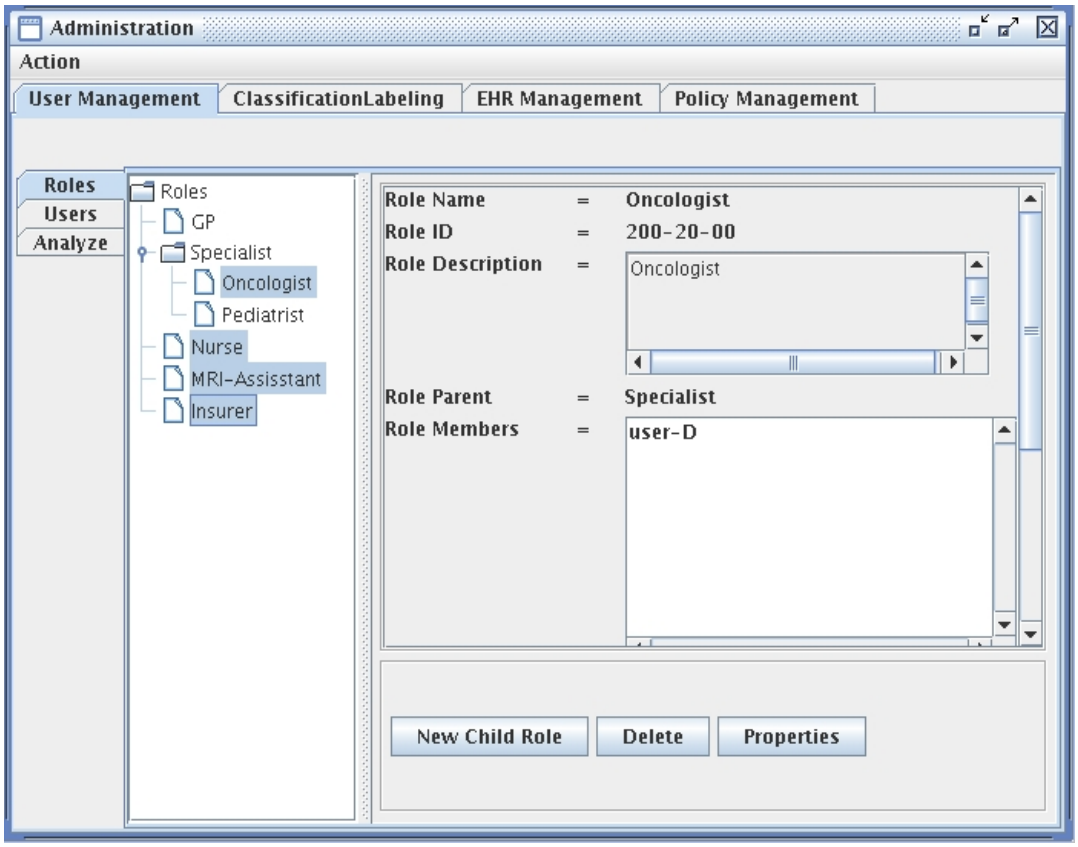

Figure 4.18: Roles of the example

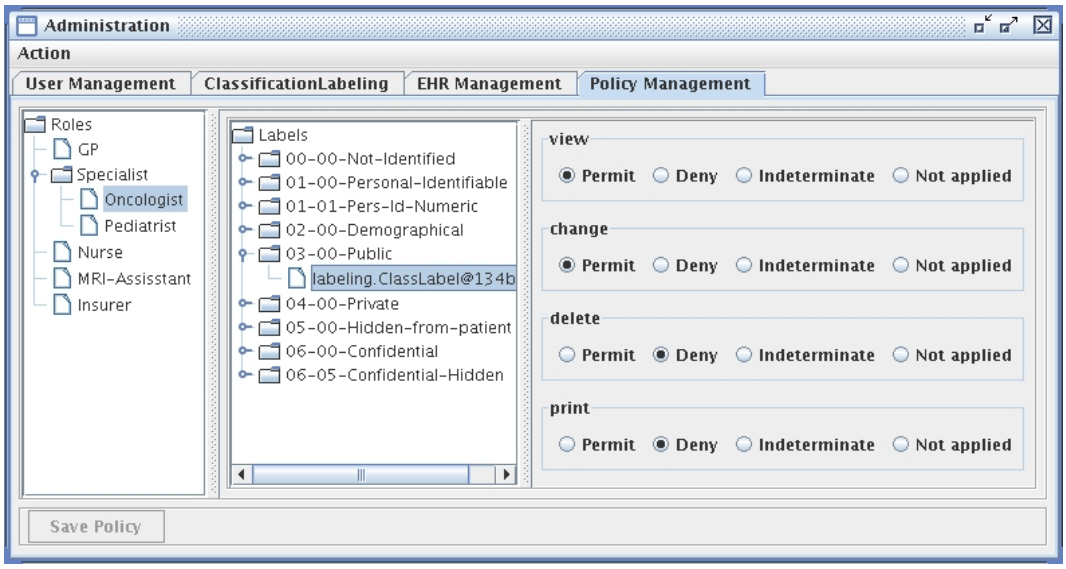

Figure 4.19: Oncologists' access rights to “Public” class

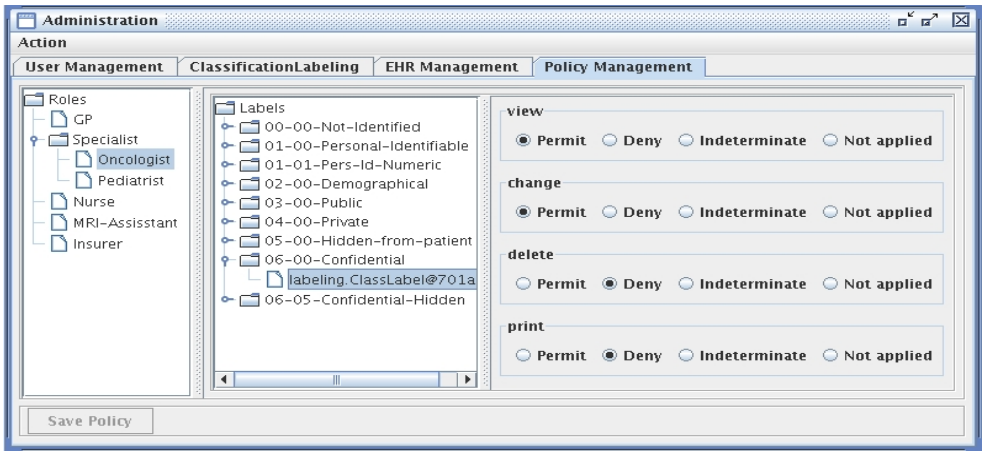

Figure 4.20: Oncologists' access rights to “Confidential” class

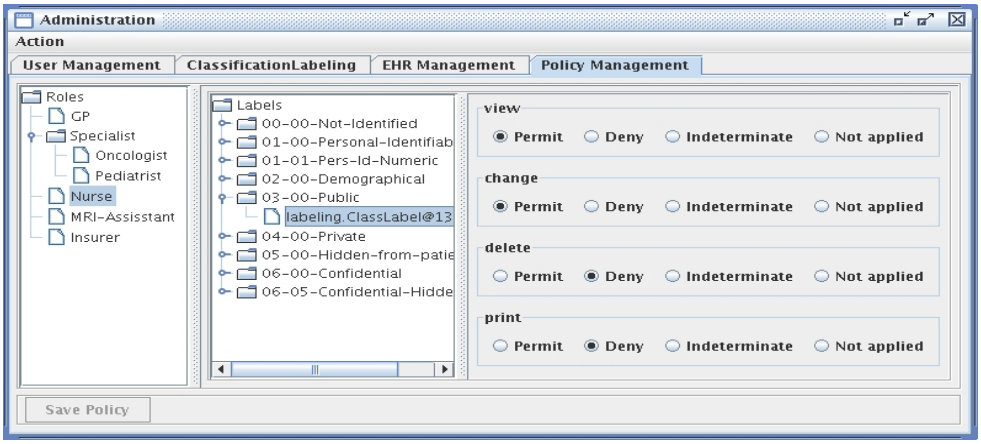

Figure 4.21: Nurses' access rights to “Public” class

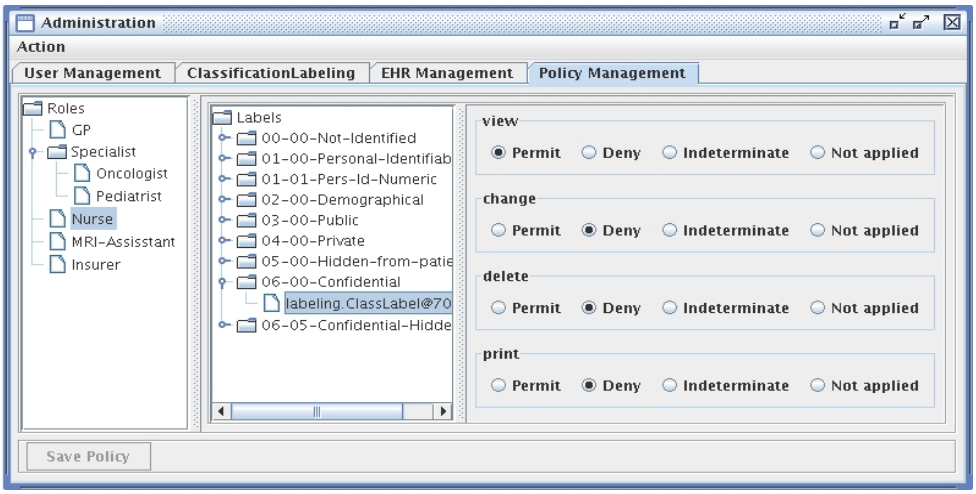

Figure 4.22: Nurses' access rights to “Confidential” class

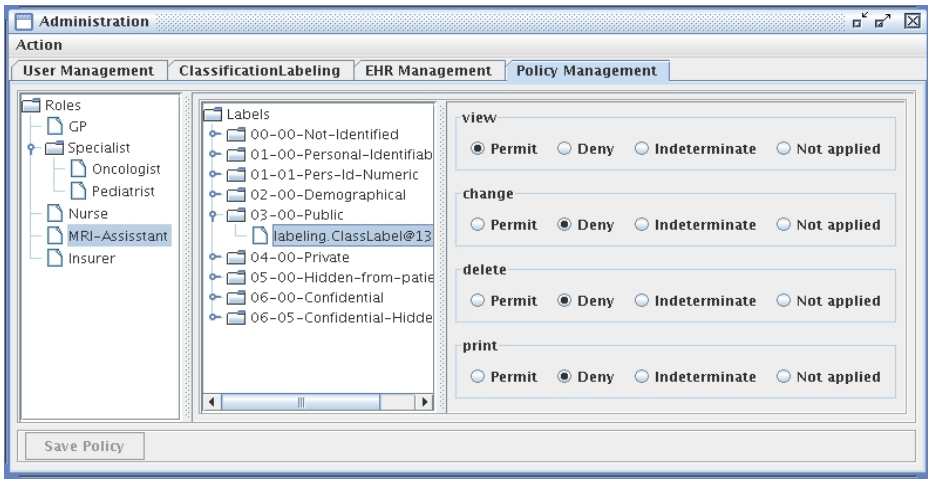

Figure 4.23: MRI assistants' access rights to “Public” class

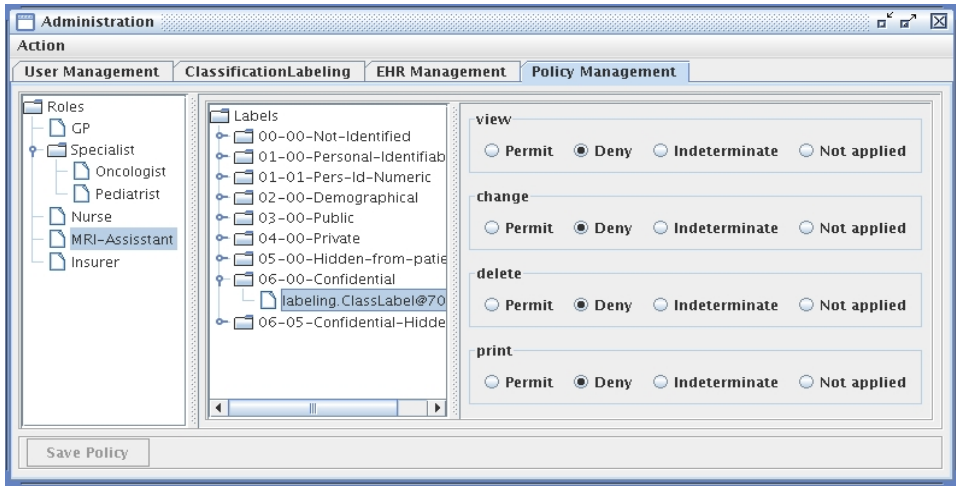

Figure 4.24: MRI assistants' access rights to “Confidential” class

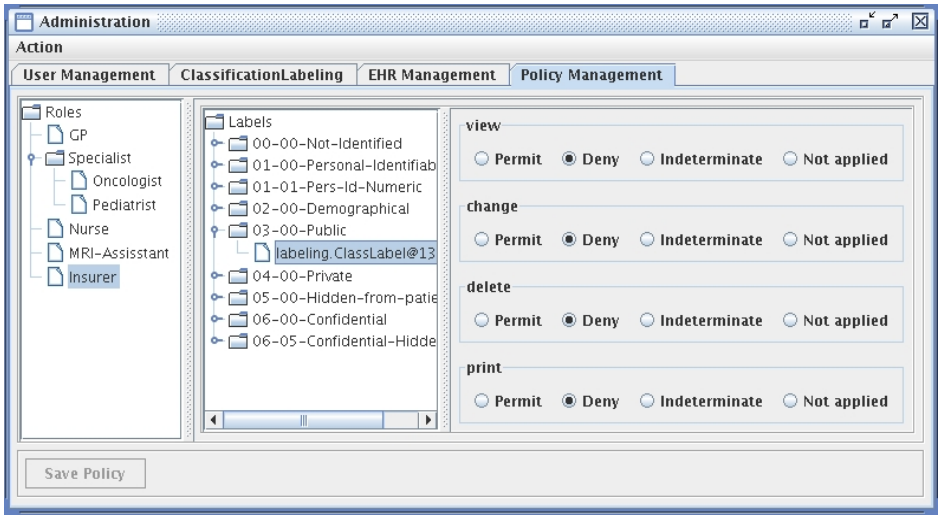

Figure 4.25: Insurers' access rights to “Public” class

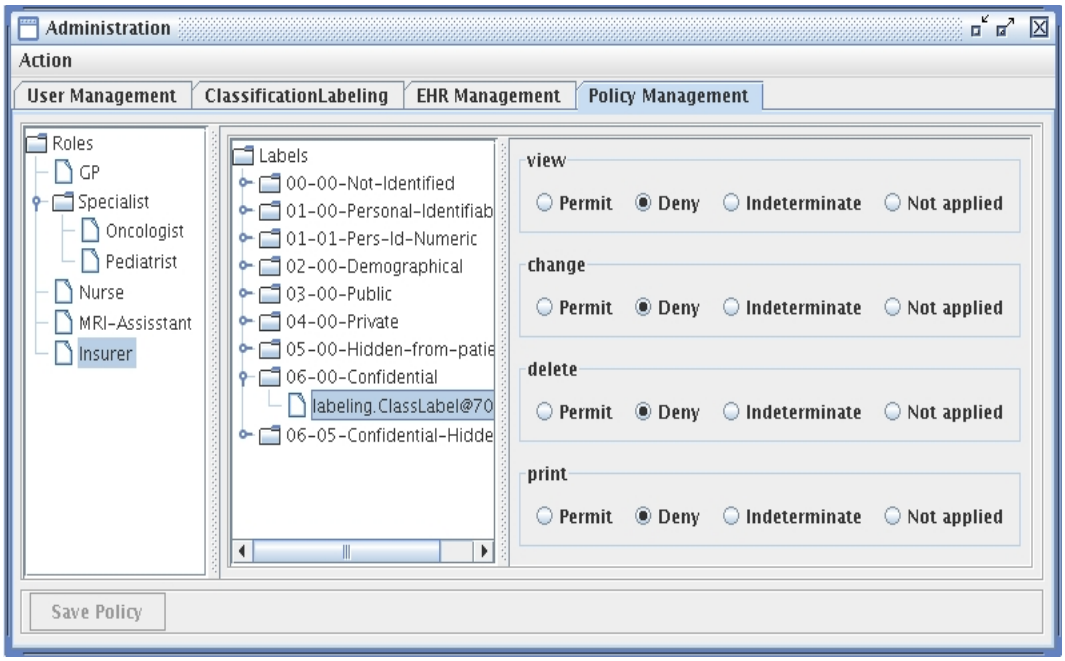

Figure 4.26: Insurers' access rights to “Confidential” class

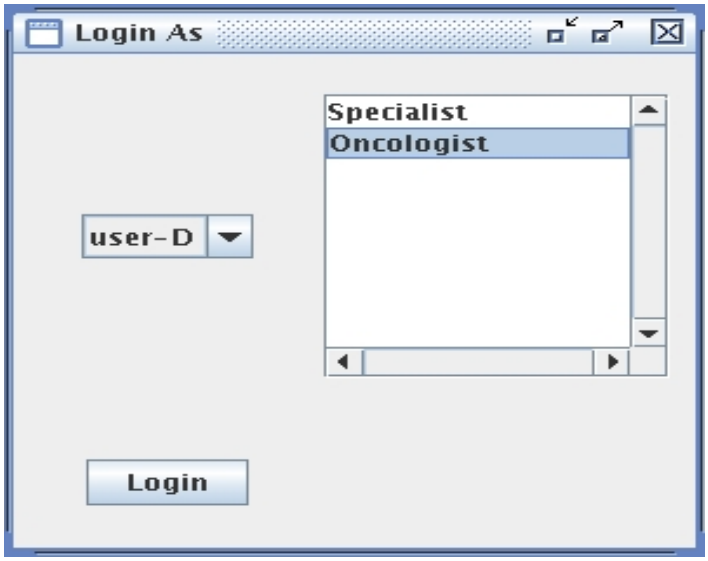

Figure 4.27: User-D logs in as an Oncologist

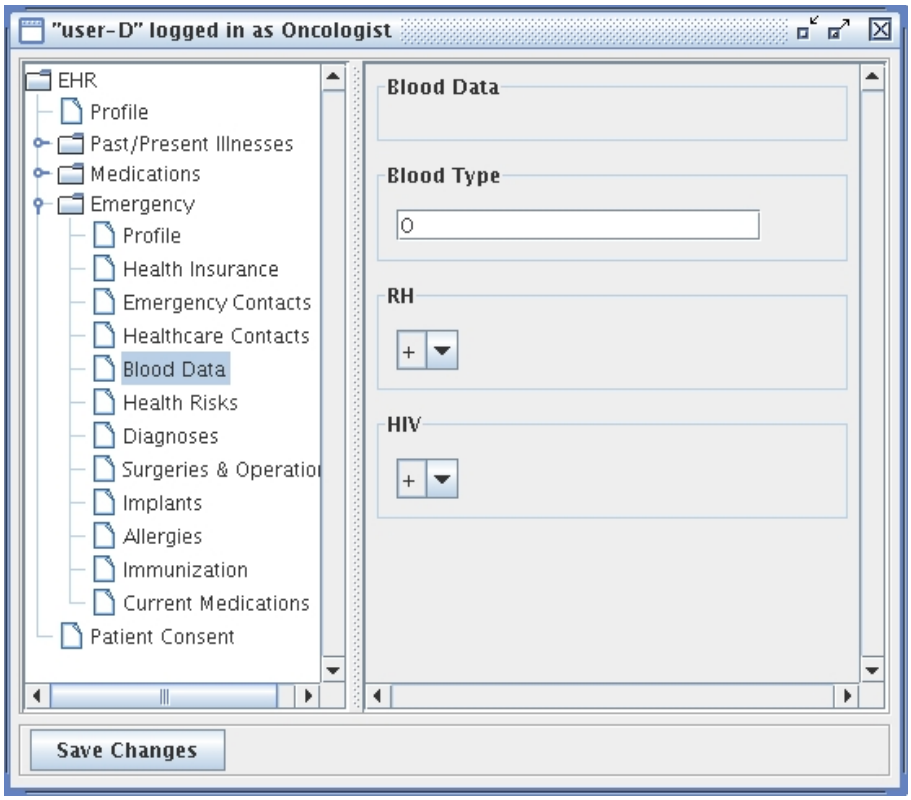

Figure 4.28: Oncologists' view of the “Blood Data”

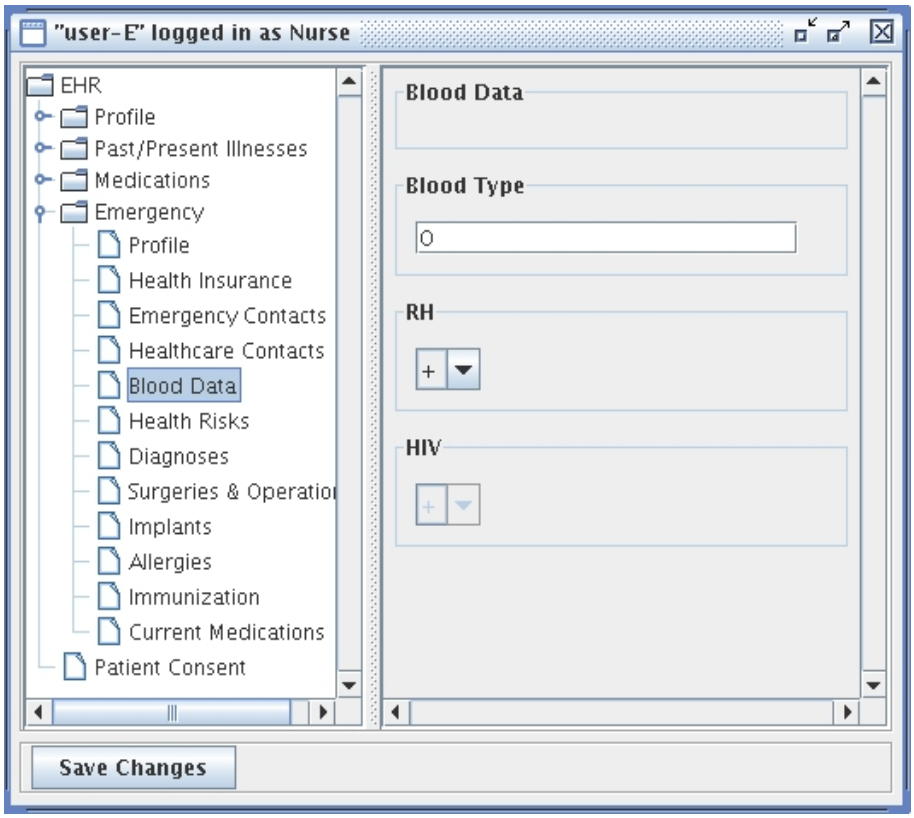

Figure 4.29: Nurses' view of the “Blood Data”

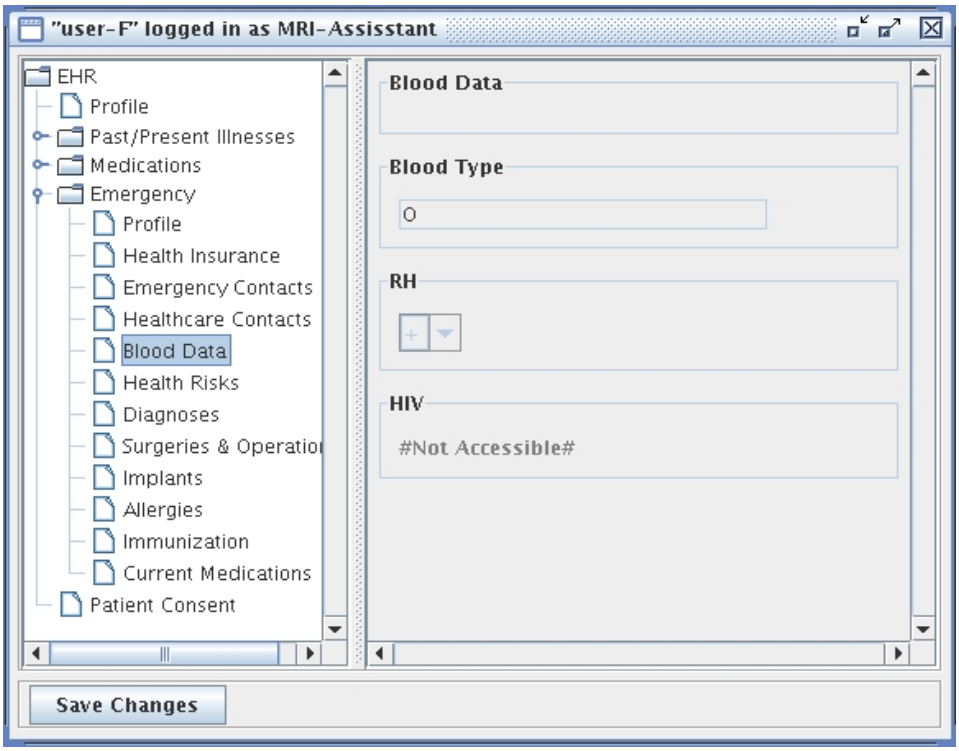

Figure 4.30: MRI-assistants' view of the “Blood Data”

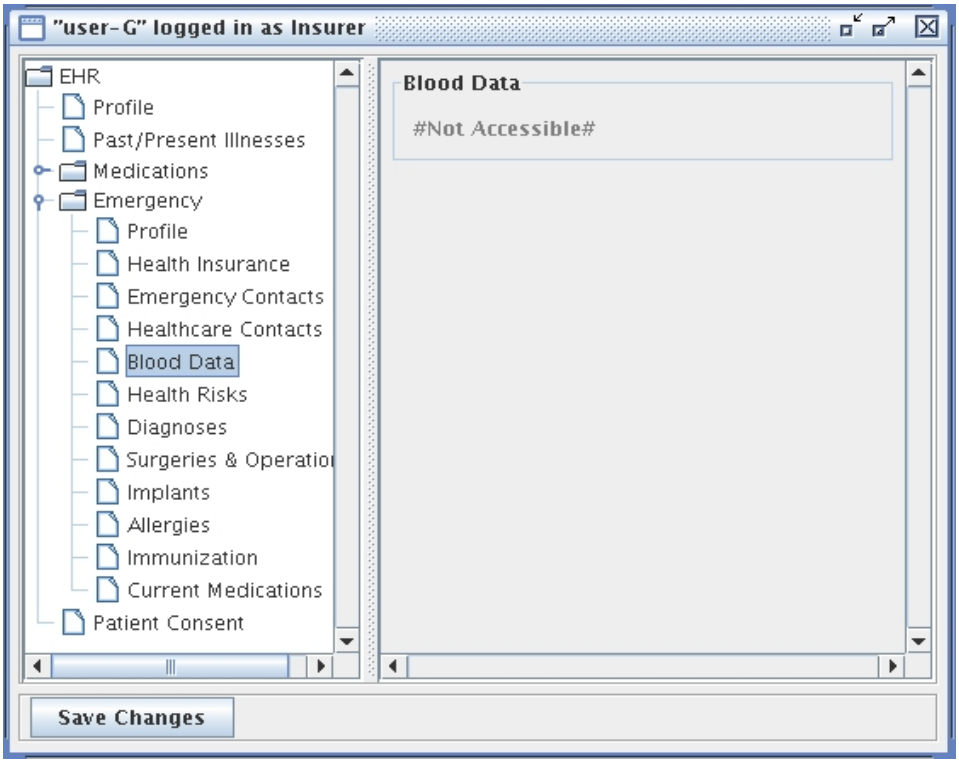

Figure 4.31: Insurers' view of the “Blood Data”

CHAPTER 5

ETHICS OF STRUCTURING PATIENT PRIVACY POLICY

5.1: Ethical Questions

During the development of S3P, we confronted with several ethical questions and problems. Below are the themes that we have constructed from our experiences with the S3P program and the questions related to them. Thus, some of the ethical questions of computerizing privacy policy can be summarized as follows. The typology of the questions we used are inspired by Anderson and Goodman [71]:

5.1.1: Need-to-know and restrictions

The main purpose of access control policy is to limit the access to the right people according to privacy policy and patient consent. Members of each role need to know a subset of EHR to accomplish their task. Highly restrictive policies are helpful in protecting privacy, however, they may affect patient safety diversely.

- What is the minimum need-to-know information for each role?
- What happens if restrictions imposed by policy prevents access to vital information?
- What happens if authorized users are not available during an emergency case?
- If it is reasonable to override restrictions to provide care, who should

initiate such overrides? Should it be done by staff on duty or by a dedicated authorized staff in HCO?

- Should patients be allowed to request customized restrictions on their EHR? For example, should they be allowed to hide their HIV status from medical staff?

5.1.2: Shared care and Granted access

In electronic healthcare, various HCOs may participate in the treatment of patients by sharing parts of their health information. To provide a high quality care the "minimum necessary" [72] information, which is the minimum subset of EHR necessary for care providing, should be specified. Additionally, physicians may need to grant access to other physicians for consultation purposes, a feature called 'Granted Access' in S3P.

- What is the minimum necessary information for each case?
- What should be done if the policy of the referred HCO is more relaxed than the policy consented by the patient in referring HCO?
- What should be done if the standards used by referring and referred entities are not compatible? What should be done if there is not a ready to use interface for checking policy protection?
- Should the HCO delay treatment to inform patients about differences in policies? If sharing is done without informing the patient, who is responsible for possible privacy violations?
- Should authorized users be allowed to transfer access rights to other physicians for consultation or collaborative care providing?
- Should the access rights of referred individual be less than the rights of referring parties?

5.1.3: Disclosure, de-identification, and re-identification

For secondary uses, such as research, disclosed information should be de-identified by removing personal identifiable parts of EHR. On the other hand, a minimum subset of data is necessary for the accuracy of research.

- What is the minimum necessary subset of EHR for research?
- Where is the balance between protecting patient privacy by de-identification and preserving the accuracy of research?
- What should be done if the location of the patient is necessary for epidemiological research? What is the minimum number of disclosed records to protect patient anonymity if location is not hidden?
- In which situations the EHR can be disclosed without informing the patients? Should patients be informed later about such disclosures?
- Is it ethical to disclose patient information regardless of their consent for public benefits, such as dealing with domestic violence?
- Should these kind of disclosures be audited?

To prevent duplication of records and for the accuracy of research, disclosed records should be uniquely identified without making the record owners known to others. Additionally, de-identification may need to be reversible, which is called re-identification, for instance to inform patient about a rare case of a disease found during research.

- What is the impact of duplication on the accuracy of research?
- In which situations disclosed informations should be re-identified?

5.1.4: Informed Consent

Informed consents are used to inform patients about the uses and disclosures of their records. Furthermore they provide patients to specify the privacy protection level by opt-in and opt-out choices applied on policy rules. By opting-in, patients can exclusively include their records in an specific access type and by opting-out they exclusively exclude their inclusion in any information gathering and usage activity.

- Is it ethical to delay care providing when informed consent is not present?
- What happens if the patient customized consents restricts access to vital information?
- Which option of patient consent is more suitable for electronic healthcare? Opt-in, opt-out, or both?

5.1.5: Leaks in privacy policy

Policies may contain errors or conflicts which can lead to privacy violations or unavailability of necessary information. conflicts may arise due to diversity of roles and the membership of individual in possibly multiple roles.

- Should patients be informed of any abuse or leak encountered in the policy?
- Who is responsible for privacy protection? Policy makers? Application developers? Hospitals?
- Will informing these deficiencies result in patients' mistrust in health provider?
- Where is the balance between protecting privacy and timely availability of information?

5.1.6: Unique Health Identifier

Using Social Security Number as a health identifier eliminates the need for remembering several identifiers, However, its usage outside healthcare will endanger patient privacy by linking EHRs to other records, such as financial records.

- What is the best choice for Unique Health Identifier ?
- Where is the balance between ease of use and protecting privacy?

5.1.7: Patient empowerment

Patients in electronic healthcare can have access and control over their health records which is called “patient empowerment” [73].

- Which parts of EHR should be viewed by patients?
- Should patients be allowed to change parts of their EHR?
- Who is responsible if such altering endangers the patient safety?
- Should changes made by patients be reviewed by HCOs?

5.1.8: Hiding

Patients in Turkey has a right to have a copy of their own medical records according to the statue of patient rights [74] (as cited in [75]). However, some parts of EHR, such as mental health information may be necessary to be hidden from patients for their own safety.

- Is it ethical to hide some parts of health records from patients? Does that guarantee the safety of patients?
- Is it ethical to hide patient condition from them upon the request of their parents or relatives?
- Should patient be given a right to opt-out such hidings?

5.1.9: Telemedicine

High speed connections and low cost storage devices enables recording all physician-patient conversations in several formats, such as voice and video.

- Which conversations should be recorded during telemedicine care providing?
- Is it ethical to use recorded conversations against the patient in any probable litigation?
- Does recording physician-patient conversations make patient privacy

more vulnerable in telemedicine compared to other types of care providing?

5.1.10: Audits

All activities done on an EHR can be audited for later quality analyses or for possible litigations.

- How comprehensively should auditing be done?
- How long should the audits be stored?
- Should the audits be removed in face of death of the patient?
- Who should have access to audit trails?
- Should the access type of the audits be read-only?

5.2: How does S3P help in solving ethical problems of computerizing privacy policies?

Among the ethical problems we confronted during the development of S3P, only a few of them could be solved by using technical methods. To thoroughly solve the problems we have discussed so far or to assess other hidden problems, there is a need for a collaborative work of experts coming from different professional backgrounds. S3P provides a means for users to define healthcare scenarios and apply privacy policies on a fictitious EHR. S3P can be used to inform non-medical experts about aforementioned ethical problems in healthcare. Additionally, it can inform medical experts about the new challenges posed by moving toward electronic healthcare and computerized privacy policies.

CHAPTER 6

CONCLUSION, SHORTCOMINGS, FUTURE WORKS

6.1: Conclusion

As the rapid move toward electronic healthcare continues, in the near future, there will be a stronger need for structured and enforceable privacy policies to protect patient privacy adequately. The focus of this thesis is on a framework for a structured patient privacy policy (S3P). It covers the EHR, classifying and labeling the EHR, primary uses of EHR, authorization, role based access control, hierarchical and multiple roles, individual based access control, de-identification and re-identification, unique health identifier, informed consent, and accountability services of an enforceable privacy policy. We also present a prototype educational application which simulates a structured and enforceable electronic privacy policy based on XACML language. S3P prototype is designed to provide a tool to test medical scenarios and assess the effect of computerized privacy policies on healthcare processes. During the development of S3P we realized that a singular focus on technical solutions falls too short to address and solve the majority of problems. S3P can be helpful to highlight such problems so that experts coming from various professional backgrounds find the most appropriate solutions. Such a timely task facilitates designing an ethically sound privacy policy suitable for electronic healthcare.

6.2: Shortcomings:

As mentioned before, the S3P is a prototype application developed with incremental software process model. As a result, existing prototype application does not contain all the features of the S3P framework discussed in 4.3 and 4.4. It supports the following features:

- Primary authorization and access control based on RBAC.
- Non-hierarchical confidentiality classification and labeling.
- Simple de-identification based on hiding the specified confidentiality classes.
- Hierarchical roles with the ability to change the access rights of the sub-roles.
- Multiple roles which enables individuals to login as different roles simultaneously.
- Simple auditing based on the role of subject, confidentiality labels of resources, and actions.

The followings are the shortcomings of the current version of the S3P:

- The lack of actual user requirement analysis. S3P, however, can be used as a prototype to assist in eliciting the user requirements.
- Since the focus was on the privacy policy rather than on standardizing the EHR, no coding system has been used to represent the EHR.
- Although XACML supports time range as an environmental parameter of access, the context based access rights are not supported in the first version.
- The access rights are assigned by an administrator or policy maker. There is no mechanism to check or change the access rights automatically. For example, if the access right of a nurse should be changed after patient discharge, only the administrator can change the access rights of that nurse.
- Opt-in and Opt-out options are not supported.
- Lack of statistically sound de-identification mechanisms.

- UHI and re-identification are not supported.
- Auditing is limited to the subject (as role), classification label, and actions related to the access.

6.3: Future works

The following are the future works or additional increments to the S3P:

- Evaluating the S3P in an actual healthcare environment.
- Eliciting the actual user requirement for an enforceable privacy policy.
- Interfacing the XACML based and non-XACML based policies.
- A mechanism for UHI to satisfy both uniquely identifying patient and re-identification.
- Automatic access right updating according to the context of the access. The time frame context based access in XACML can be used for such updating.
- Statistically sound de-identification mechanisms.
- Two way informed consents which support both opt-in and opt-out features.
- Auditing can be enriched by the details of resource, individual identity of the subjects, and context of the access.

REFERENCES

[1] *Patient Parivacy Rights, Background* (n.d.). Retrieved August 20, 2006, from http://www.patientprivacyrights.org/site/PageServer?pagename=Background.

[2] Smith, E. & Eloff, J.H.P. (1999). Security in health-care information systems-current trends. *International Journal of Medical Informatics, 54,* 39-54.

[3] Anderson, JG. & Goodman, KW. (2002). *Ethics and Information Technology: A case-based approach to a health care system in transition*, New York: Springer-Verlog.

[4] Winkler, EC. (2005). The ethics of policy writing: how should hospitals with moral disagreement about controversial medical practices?. *Journal of Medical Ethics, 3*,559-566.

[5] *Patient Privacy Rights, True stories of medical privacy violations* (n.d.). Retrieved Augost 20, 2006, from http://www.patientprivacyrights.org/site/PageServer?pagename=PrivacyAbuseStories .

[6] *National Consumer Health Privacy Survey 2005: Executive Summary* (n.d.) Retrieved Augost 20, 2006, from http://www.chcf.org/topics/download.cfm?pg=ihealth&fn=ConsumerPrivacy2005ExecSum%2Epdf&pid=438594&itemid=115694.

[7] Sadan, B. (2001). Patient data confidentiality and patient rights. *International Journal of Medical Informatics, 62*,41-49.

[8] *Privacy* (n.d.). Retrieved August 22, 2006, from http://en.wikipedia.org/wiki/Privacy.

[9] Rada, R. (2003). *HIPAA@IT Essentials: Health Information Transactions, Privacy, and Security, 2nd Edition*. Baltimore: HIPAA-IT LLC

[10] *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July, 1973. chapter III, Safeguards for Privacy.* (n.d.) Retrieved Augost 22, 2006, from http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[11] *Marriam-Webster Online, Policy.* (n.d.). Retrieved August 22, 2006, from http://www.webster.com/cgi-bin/dictionary?sourceid=Mozilla-search&va=policy.

[12] Blobel, B. & France, FR. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics*, 62, 51-78.

[13] *Toward a New Health Care System THE CIVIL LIBERTIES ISSUES IN BRIEF Summary of an ACLU Pub.* (n.d.). Retrieved August 22, 2006, from http://www.skepticfiles.org/aclu/health_s.htm.

[14] Barrows, RC. & Clayton, PD. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, 3(2), 139-148.

[15] *Glossary of Common Terms, Health Insurance Portability and Accountability Act of 1996 (HIPAA).* (n.d.). Retrieved August 22, 2006, from http://healthcare.partners.org/phsirb/hipaaglos.htm#g40.

[16] *TalkBank, Part I: Explanation of Informed Consent.* (n.d.). Retrieved August 22, 2006, from http://talkbank.org/share/consent.html.

[17] *ETHICS IN MEDICINE, University of Washington School of Medicine, Informed Consent.* (n.d.). Retrieved August 23, 2006, from http://depts.washington.edu/bioethx/topics/consent.html.

[18] *Informed Consent.* (n.d.). Retrieved August 22, 2006, from http://www.ama-assn.org/ama/pub/category/4608.html

[19] *Patients Rights and Informed Consent*. (n.d.). Retrieved August 22, 2006, from http://www.spineuniverse.com/displayarticle.php/article2463.html

[20] *What were the major modifications to the HIPAA Privacy Rule that were adopted in August 2002?*. Retrieved August 22, 2006, from http://healthprivacy.answers.hhs.gov/cgi-bin/hipaa.cfg/php/enduser/popup_adp.php?p_sid=KRQmubhi&p_lva=&p_li=&p_faqid=192&p_created=1040314104&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PWRmbHQmcF9ncmlkc29ydD0mcF9yb3dfY250PTIwJnBfcHJvZHM9JnBfY2F0cz03LDAmcF9wdj0mcF9jdj0xLjc7Mi51MCZwX3NlYXJjaF90eXBlPWFuc3dlcnMuc2VhcmNoX25sJnBfcGFnZT0xJnBfc2VhcmNoX3RleHQ9Y29uc2VudA.

[21] *Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?*. (n.d.). Retrieved August 22, 2006, from http://healthprivacy.answers.hhs.gov/cgi-bin/hipaa.cfg/php/enduser/std_adp.php?p_faqid=193&p_created=1040314178&p_sid=KRQmubhi&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PWRmbHQmcF9ncmlkc29ydD0mcF9yb3dfY250PTIwJnBfcHJvZHM9JnBfY2F0cz03LDAmcF9wdj0mcF9jdj0xLjc7Mi51MCZwX3NlYXJjaF90eXBlPWFuc3dlcnMuc2VhcmNoX25sJnBfcGFnZT0xJnBfc2VhcmNoX3RleHQ9Y29uc2VudA**&p_li=&p_topview=1.

[22] Reed, A. (2005, January). What Privacy?. *DigitalIDWorld, Jan/Feb 2005*, 72, 68-70.

[23] List, JM. (2004). “Opting-In” and Unnecessary Penalties for Non Kidney Donors. *American Journal of Bioethics, 4(4)*, 39-41.

[24] Walsmley, S. (2003). Opt in or opt out: What is optimal for prenatal screening for HIV infection?. *Canada's Leading Medical Journal, 168(6),* 707-708.

[25] Lo, B., Wolf, L. & Sengupta, S. (2000). Ethical issues in early detection of HIV infection to reduce vertical transmission. *Journal of Acquired Immune Deficiency Syndromes, 25(Suppl 2)*, S136-43.

[26] Kahneman, D. & Tversky, A. (1984). “Choices, values, and frames.” American *Psychologist, 39(4),* 341-350.

[27] Bellman,S., Johnson, EJ. & Lohse, GL. (2001). On Site: To opt-in or opt-out? it depends on the question. *Communications of the ACM, 44,* 25-27, Retrieved August 24, 2006, from http://delivery.acm.org/10.1145/360000/359241/p25-bellman.html?key1=359241&key2=7641808511&coll=portal&dl=ACM&CFID=11111111&CFTOKEN=2222222.

[28] *HIPAA FAQ: Unique Identifiers* (n.d.). Retrieved August 23, 2006, from http://www.hipaadvisory.com/action/faqs/FAQ_Identifiers.htm.

[29] *Unique Health Identifier for Individuals* (n.d.). Retrieved August 23, 2006, from http://www.hipaanet.com/UHI-2.htm.

[30] *U.S. Department of Health and Human Services, Unique Health Identifier for Individuals, A White Paper* (n.d.). Retrieved August 23, 2006, from http://www.epic.org/privacy/medical/hhs-id-798.html.

[31] *National Information Assurance Glossary, CNSS Instruction No. 4009, Revised June 2006.* (n.d.). Retrieved August 23, 2006, from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[32] Krutz, RL. & Vines, RD. (2001). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security.* New York: John Wiley & Sons, Inc.

[33]Sandhu, R.S. & Samarati, P. (1994, September). Access Control: Principles and Practice. *Communications magazine, IEEE, 32(9)*, 40-48.

[34] *De-Identification.* (n.d.). Retrieved August 24, 2006, from http://www.mii.ucla.edu/DataServer/docs/features/deidentification.html

[35] Duncan GT. (2002). Policy and practice on release of microdata, *Proceedings of the 19th CEIES Seminar, "Innovative Solutions in Providing Access to Microdata.,* 15-22. Retrieved August 23, 2006, from http://forum.europa.eu.int/Public/irc/dsis/ceies/library?l=/seminars_11_to_20/innovative_solutions/english_documents/en_final_pdf/_EN_1.0_&a=d#search=%22Census%20Microdata%20Unit's%20Samples%20of%20Anonymised%20Records'%20(SARs)%20protection%20measures%20deidentification%22

[36] *Reidentification of Individuals in Chicago's Homicide Database, A Technical and Legal Study* (n.d.). Retrieved August 24, 2006, from http://web.mit.edu/sem083/www/assignments/reidentification.html.

[37] *HIPAA privacy manual: De-identification and Re-identification.* (n.d.). Retrieved August 24, 2006, from http://www4.utsouthwestern.edu/hipaa/Policy%205_1.htm

[38] *EHR Privacy and Security Requirements, Reference: Electronic Health Record(EHR) Privacy and Security Requirements, February 7, 2005* (n.d.). Retrieved Augost 21, 2006, from
http://www.nlchi.nf.ca/pdf/PPIA_Appendix_B.pdf

[39] Goldman, J., Hudson, Z., Smith, R.(2000). *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*. Retrieved August 20, 2006, from Publication of the AAAS Scientific Freedom, Responsibility and Law Program, in collaboration with the Committee on Scientific Freedom and Responsibility Professional Society Ethics Group Web site:
http://www.aaas.org/spp/sfrl/per/per20.htm

[40] Rosati, K. (2002). DHHS wisely proposed to remove the "consent" requirement from the HIPAA privacy standards. Department of Health and Human Services. *Journal of Health Law, 35(3)*,395-402. Retrieved September 1, 2006, from PubMed database.

[41] Reed, A. (February 2005). What privacy?. *Digital ID World, January/February 2005*, 72,68-70

[42] *Glossary of sensemaking terms* (n.d.). Retrieved August 20, 2006, from
http://www2.parc.com/istl/groups/hdi/sensemaking/glossary.htm

[43] *Healthcare Information and Management Systems Society, EHR* (n.d.). Retrieved August 20, 2006, from
http://www.himss.org/ASP/topics_ehr.asp

[44] Waegemann Peter, C. *Status Report 2002: Electronic Health Records* (n.d.). Retrieved August 20, 2006, from
http://www.medrecinst.com/uploadedFiles/MRILibrary/StatusReport.pdf

[45] Upham, R. (2004). *The Electronic Health Record: Will It Become a Reality?*, Retrieved August 20, 2006, from
http://www.hipaadvisory.com/action/ehealth/EHR-reality.htm

[46] *Health Care Decision Making* (n.d.). Retrieved August 21, 2006, from
http://www.dartmouth.edu/~cecs/decision_making.html

[47] Muramoto, O. (2001). Bioethical aspects of the recent changes in the policy of refusal of blood by Jehovah's Witnesses. *British Medical Journal, 6*, 322(7277),37-39. Retrieved September 1, 2006, from PMC database.

[48] Truog, RD. & Robinson, WM. (2003). Role of brain death and the dead-donor rule in the ethics of organ transplantation. *Critical Care Medicine, 31(9)*,2391-2396.

[49] Cohen, JS., Fihn, SD., Boyko, EJ., Jonsen, AR. & Wood, RW. (1994). Attitudes toward assisted suicide and euthanasia among physicians in Washington state. *The New England Journal of Medicine. 331*:89–94.

[50] Staber, R., Aden, T. & Eichelberg, M. (2006, June). *Enabling cross-organization access to legacy healthcare information systems in ARTEMIS using the IHE RID profile.* Paper presented at the 24th International EuroPACS conference, Trondheim, Norway.

[51] Rosati, K. (2002). DHHS wisely proposed to remove the "consent" requirement from the HIPAA privacy standards. Department of Health and Human Services. *Journal of Health Law, 35(3)*, 395-402.

[52] Walt, C. V. D. (2001, October 9). *Introduction to Security Policies, Part Three: Structuring Security Policies*. Retrieved August 24, 2006, from http://www.securityfocus.com/infocus/1487

[53] *Sun's XACML Implementation, Programmer's Guide for Version 1.2* (n.d.). Retrieved August 10, 2006, from http://sunxacml.sourceforge.net/guide.html#xacml.

[54] Verma, M. (2004, October 18). *XML Security: Control information access with XACML.* Retrieved August 10, 2006, from http://www-128.ibm.com/developerworks/xml/library/x-xacml/

[55] Bertino, E. *Security of distributed systems.* (n.d.). Retrieved August 10, 2006, from http://homes.cerias.purdue.edu/~bhargav/cs526/security-11.ppt

[56] Walsh, N. (1998, October 03). *A technical introduction to XML.* Retrieved August 11, 2006, from http://www.xml.com/pub/a/98/10/guide0.html

[57] *Platform for Privacy Preferences (P3P) Project, Enabling smarter Privacy Tools for the Web.* (n.d.). Retrieved August 11, 2006, from http://www.w3.org/P3P/.

[58] Stufflebeam, WH., Antón, AI., He, Q. & Jain, N.(2004). **S**pecifying privacy policies with P3P and EPAL: lessons learned. *Workshop On Privacy In The Electronic Society, Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, 35.

[59] Liu, L., Yu, E. & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International,* 105 – 114.

[60] *The Enterprise Privacy Authorization Language (EPAL 1.1) - Reader's Guide to the Documentation.* (n.d.). Retrieved August 13, 2006, from http://www.zurich.ibm.com/security/enterprise-privacy/epal/.

[61] Ashley, P., Hada, S., Karjoth, G., Powers, C. & Schunter, M. (2003). *Enterprise Privacy Authorization Language (EPAL 1.1)*, Retrieved August 13, 2006, from http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html.

[62] Ashley, P., Hada, S., Karjoth, G., Powers, C. & Schunter, M. *The Enterprise Privacy Authorization Language (EPAL)- How to Enforce Privacy throughout an Enterprise*, (n.d.). Retrieved August 13, 2006, from http://www.w3.org/2003/p3p-ws/pp/ibm3.html#_ftnref5.

[63] Anderson, A. *A Comparison of Two Privacy Policy Languages: EPAL and XACML*. (n.d.). Retrieved August 14, 2006, from http://research.sun.com/techrep/2005/smli_tr-2005-147/TRCompareEPALandXACML.html.

[64] Mont, MC. & Thyne, R. (2006, June). *A Systemic Approach to Automate Privacy Policy Enforcementin Enterprises*, 6th Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge, United Kingdom

[65] Sommerville, L. (2004). *Software engineering.* Boston: Pearson/Addison-Wesley.

[66] *LifeSensor! Welcome Bob Jones.* (n.d.). Retrieved August 24, 2006, from https://record.de.lifesensor.com/nav/shell_tree.jsp#pagetop.

[67] *CERN Engineering Data Management Service, Engineering Data Management*

Glossary. (n.d.). Retrieved August 24, 2006, from http://cedar.web.cern.ch/CEDAR/glossary.html#Classification.

[68] Ferraiolo, D.F., Kuhn, D.R., & Chandramouli, (2003). R. *Role Based Access Controls,* Boston: Artech House.

[69] Barkley, J. *Role Based Access Control.* (1995). Retrieved August 25, 2006, from http://hissa.nist.gov/rbac/proj/paper/node3.html.

[70]*Research Repositories, Databases, and the HIPAA Privacy Rule.* (n.d.). Retrieved August 25, 2006, from http://privacyruleandresearch.nih.gov/research_repositories.asp.

[71] *JAVA SE downloads.* (n.d.). Retrieved August 23, 2006, from http://java.sun.com/javase/downloads/index.jsp.

[72] *Sun's XACML implementation.* (n.d.). Retrieved August 23, 2006, from http://sunxacml.sourceforge.net/.

[71] Anderson, JG. & Goodman, KW. (2002). *Ethics and Information Technology: A case-based approach to a health care system in transition. In: Introduction: Case Studies in Ethics and Health Informatics.* New York: Springer-Verlog.

[72] Aikins, R. *HIPAA- Minimum necessary.* (n.d.). Retrieved August 16, 2006, from http://www.oahhs.org/issues/hipaa/minimum_necessary.php.

[73] Munir, S. & Boaden, R. (2001). Patient empowerment and the electronic health record. *Studies in Health Technology and Informatics, 84,* 663-665.

[74] T.C.Sağlık Bakanlıgı. (1998). *Hasta Hakları Yönetmenliği* (R.G. Sayısı:23420).

[75] Aydin, E. (2004). Rights of patients in developing countries: the case of Turkey. *Journal of Medical Ethics, 30,* 555-557.

APPENDICES

APPENDIX A: SUTTER LAKESIDE HOSPITAL NOTICE OF PRIVACY PRACTICES

Sutter Lakeside Hospital

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED BY SUTTER LAKESIDE HOSPITAL AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

What is this Notice and Why it is Important

This notice is required by law to inform you of how your health information will be protected, how Sutter Lakeside Hospital (SLH) may use or disclose your health information, and about your rights regarding your health information. If you have any questions about this notice, please contact SLH Privacy Officer at 707/262-5066, extension 5371.

Understanding Your Health Information

Each time you visit a physician, healthcare provider or hospital, a record of your visit is made. Typically, this record contains a description of your symptoms, medical history, examination and test results, diagnoses, treatment, and a plan for future care. This information, often referred to as your medical record, serves as a:

- Basis for planning your care and treatment
- Means of communication among the health professionals who contribute to your care

• Legal documents of the care you receive

• Means by which you or a third-party payer (e.g. health insurance company) can verify that services you received were appropriately billed

• A data source for medical research and public health

• A source of data for planning facilities, marketing healthcare services, and fundraising

• A tool for educating health professionals

• A tool with which we can assess and work to improve the care we provide Understanding what is in your record and how your health information is used helps you to ensure its accuracy; better understand how others may access and use your health information; and make more informed decisions when authorizing disclosures to others.

Your Health Information Rights

You have the following rights related to your medical and billing records kept by SLH:

Obtain a copy of this notice. You will receive a copy of this notice at your first visit after its publication. Thereafter you may request a copy of this notice or any revisions from the Information Desk, from our website www.lakeside.sutterhealth.org or by calling 707/262- 5373.

Authorization to use your health information. Before we use or disclose your health information, other than as described below, we will obtain your written authorization, which you may revoke at any time to stop future use or disclosure.

Access to your health information. You may request a copy of your health information that SLH keeps in your medical or billing record. Your request must be submitted in writing. We may charge for the costs of providing you access and for your copies.

Amend your health information. If you believe the information we have about

you is incorrect or incomplete, you may request that we correct or add information. Your request must be in writing and you may pick up a form for this purpose in the Health Information Management (Medical Records) Department.

Request confidential communications. You may request that, when we communicate with you about your health information, we do so in a specific way (e.g. at a certain mail address or phone number). We will make ever reasonable effort to agree to your request.

Limit our use or disclosure of your health information. You may request in writing that we restrict the use or disclosure of your health information for treatment, payment, health care operations, or any other purpose except when specifically authorized by you, when we are required by law, or in an emergency situation in order to treat you. We will consider your request and respond, but we are not legally required to agree if we believe your request would interfere with our ability to treat you or collect payment for our services.

Accounting of disclosures. You may request a list of disclosures of your health information that we have made for reasons other than treatment, payment or healthcare operations. Disclosures that we make with your authorization will not be listed. We will provide one list per year free of charge, but may charge for subsequent lists in the same year.

Our Responsibilities

We are required by law to protect the privacy of your health information, establish policies and procedures that govern the behavior of our workforce and businesses associates, and provide this notice about our privacy practices, and abide by the terms of this notice.

We reserve the right to change our policies and procedures for protecting health information. When we make a significant change in how we use or disclosure your health information, we will also change this notice. The new notice will be posted in the waiting and admission areas, on our website, and will be available at the information desk.

Except for the purposes related to your treatment, to collect payment for our services, to perform necessary business functions, or when otherwise permitted or required by law, we will not use or disclose your health information without your authorization. You have the right to revoke your authorization at any time. We are unable to take back any disclosure we have already made with your permission.

Examples of Uses and Disclosures for Treatment, Payment and Healthcare Operations

We will use your health information to facilitate your medical treatment.

For example: Information obtained by a nurse, physician, or other members of your healthcare team will be recorded in your record and used to determine the course of your medical treatment. Your provider may document in your record his or her expectations of the members of your healthcare team. Members of your healthcare team will then record the actions they take and their observations as appropriate. In that way, the physician will know how you are responding to treatment. We will also provide your physician, or other healthcare providers involved with your treatment (e.g. specialists, consulting physicians, anesthesiologists, therapists, etc.) with copies of various reports that should assist them in treating you.

We will use your health information to collect payment for health care services that we provide.

For example: A bill may be sent to you or your health insurance company. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis, procedures and supplies used. In some cases, information from your medical record is sent to your insurance company to explain the need for or provide additional information about your treatment.

We will use your health information to facilitate routine healthcare operations.

For example: Members of our medical staff or quality improvement teams may use

information in your record to assess the care you have received and how your

progress compares to others. This information will then be used in efforts to improve the quality and effectiveness of the healthcare and other services we provide. SLH is an affiliate of the Sutter Health network. We may permit Sutter Health to use your health information to support necessary business, financial, and clinical functions. Examples of these functions may include: auditing our clinical procedures, analyzing our cost of care, arranging for patient satisfaction surveys, and determining the need for new healthcare services.

We will use your health information to help us educate medical staff, residents, and students.

For example: SLH has associations with a variety of schools involved in the education of health professionals. All staff, residents, and students must sign a confidentiality agreement before accessing any health information maintained by SLH.

We will use your health information to notify your family and friends about your condition.

For example: We may use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care or your general condition. Health professionals, using their best judgment, may disclose to a family member, other relative, close personal friend or any other person you identify, relevant health information to facilitate the person's ability to assist in your care or make arrangements for payment of your care.

We may use your health information to inform persons about your death.

For example: We may disclose health information to funeral directors, coroners, and medical examiners consistent with applicable law to carry out their duties.

Examples of Uses and Disclosures for Other Purposes

Appointment Reminders: We may contact you to provide appointment reminders.

Alternative Treatments: We may use your health information to provide you with information about alternative treatments such as acupuncture, biofeedback, massage therapy, stress reduction.

Directory Information: We may include your name, location, and general condition (e.g. fair, stable, critical) and your religious affiliation in our directory information. This information is used to assist persons who wish to visit you, deliver gifts, or inquire about your condition. We will give you an opportunity to restrict this information.

Marketing: We may use your health information to inform you about our healthcare services, treatment alternatives or other health-related benefits and services that may be of interest to you. We may also inform you about commercial products or services when we think they would be of interest to you, if you have authorized us to do so.

Fundraising: We are a community-based, not-for-profit medical center that depends extensively on charitable support. We may use limited information about you such as your name, address, demographic information, and the dates you received treatment , and we may disclose this information to SLH fundraising foundation to inform you of opportunities to support SLH and its services and programs.

Research: We may contact you to request your participation in an authorized research study. If the study provides any type of healthcare treatment, the researcher will explain the benefits and risks of the treatment, how your health information will be used during the course of the study, and whether any of your health information rights are affected. You will need to authorize the use of your health information and agree to any suspension of your rights to participate in the study, however you may revoke this authorization at any time. In some cases, we may disclose your health information to researchers when an institutional review or privacy board has approved their research. Prior to giving any information, special procedures will be

established to protect the privacy of your information.

Workers compensation: We may disclose your health information to the extent authorized by and necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Organ procurement organizations: Should you be an organ or tissue donor, we may disclose your donor status and health information to organizations engaged in the procurement, banking, or transplantation of organs, consistent with applicable laws.

Public health: We may disclose your health information as required by law to public health or legal authorities charged with preventing or controlling disease, injury or disability.

To avert a serious threat to health or safety: We may use and disclose your health when necessary to prevent a serious threat to your health and safety or to the health and safety of the public or another person. Any disclosure would be made only to someone able to help prevent the threat.

Correctional institution: Should you be an inmate of a correctional institution, we may disclose to the institution or their agents health information necessary for your health and the health and safety of other individuals.

Law enforcement: We may disclose your health information for law enforcement purposes as required by law or in response to a valid subpoena, or court or administrative order.

Food and Drug Administration (FDA): We may disclose to the FDA your health information relating to adverse events with respect to food, nutritional supplements, products and product defects, or post-marketing surveillance information to enable product recalls, repairs or replacement.

Device Manufactures: If you receive a medical device that is implanted or which is used to for life support functions, we may disclose your name, address and other information as required by law to the device manufacturer for tracking purposes. You may refuse to authorize the disclosure of your name and contact information.

Business associates: There are some services provided in our organization through contracts with business associates. Examples include transcribing your medical record, surveying for patient satisfaction, and a copy service we use when making copies of your health record. When these services are provided by contracted business associates, we may disclose the appropriate portions of your health information to our business associates so they can perform the job we have asked them to do. To protect your health information, however, we require all business associates to sign a confidentiality agreement verifying they will appropriately safeguard your information.

Special Situations

Military and Veterans: If you are a member of the armed forces, we may disclose your health information as required by military command authorities. We may also disclose health information about foreign military personnel to the appropriate foreign military authority.

National Security and Intelligence Activities: We may disclose your health information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Protective Services for the President and Others: We may disclose your health information to authorized officials so they may provide protection to the President and other governmental leaders, or conduct special investigations.

Regulatory oversight: We may disclose your health information to appropriate health oversight agencies, public health authorities or attorneys, when required by

law. Your health information may also be disclosed if a workforce member or business associate believes in good faith that SLH has engaged in unlawful conduct or has otherwise violated professional or clinical standards and are potentially endangering one or more patients, workers or the public.

For More Information or to Report a Problem

If you have questions, would like additional information, or want to request an updated copy of this notice, you may contact the SLH Privacy Officer at 707/262-5066 extension 5371.

If you believe we have not properly protected your privacy, have violated your privacy rights, or you disagree with a decision we have made about your rights, you may contact SLH's Privacy Officer. You may also send a written complaint to the U.S. Department of Health and Human Services at Hubert H. Humphrey Building, 200 Independence Avenue S.W., Room 509 HHH Building, Washington, D.C. 20201. SLH will ensure that the care you receive at our facility will in no way be impacted if you file a complaint.

Each organization listed below agrees to follow the practices described in this Notice.

Sutter Lakeside Hospital, Family Birthing Center, Upper Lake Community Health Center, Urgent Care Clinic, Family Medicine Clinic, Sutter Lakeside Home Medical Services, Sutter Lakeside Cardiac Rehabilitation Center, Sutter Lakeside Occupational Health Center, Sutter Lakeside Wellness Center.

APPENDIX B: KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ POLİTİKASI

T.C.
SAĞLIK BAKANLIĞI
Bilgi İşlem Daire Başkanlığı

1. Amaç

Bu politikanın amacı Sağlık Bakanlığı bütün kurum ve kuruluşlarının (merkez ve taşra teşkilatları, hastaneler, sağlık ocakları, aile hekimleri vs.) hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken kuralları tanımlamaktır. Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, grafik imajları, fatura gibi konular girmektedir.

2. Kapsam

Bu politika Sağlık Bakanlığı bütün kurum ve kuruluşları (merkez ve taşra teşkilatları, hastaneler, sağlık ocakları, aile hekimleri vs.) çalışanlarını kapsamaktadır.

3. Politika

3.1. Genel Kurallar

- 1. Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.
- Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlik, bütünlük ve erişilebilirliktir.
- Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.

- Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
- Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
- Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
- Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
- Hasta dosyasının bir kopyası hastaya teslim edilmelidir. Hiçbir hasta kaydı, elektronik veya kağıt ortamında [Bakanlığımızın bu konularda çıkardığı genelgeler hariç] hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilemez. (Yürürlükteki genelgelere göre Hasta Sağlık bilgilerini Sosyal Güvence Kurumları (Bağkur, SSK, ES, GSS) elde edebilir. Özel sigorta kurumları hastanın sağlık bilgilerini elde edemez.
- Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]
- Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
- Bütün hasta sağlık sağlık kayıtları fiziksel olarak korunmuş mekanlarda saklanmalıdır.
- Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.
- Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir. Bu durumda

hasta sağlık bilgisi hasta tanımlayıcısı ile ilişkilendirilemez.

3.2 Sistem Güvenliği

- Veriye erişirken dört temel prensibin gerçekleştirilmesi gerekmektedir. Bunlar; İzlenebilirlik, kimlik sınama, güvenirlik ve inkar edilememedir.
- Sağlık kurumları bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Veri tabanlarında hiçbir zaman hastalık tanısı ile TC kimlik numarası eşleşmeyecek, TC kimlik numarasından tek yönlü algoritma ile türetilmiş özel bir tanımlayıcı numara kullanılacaktır.
- Bilgi sistemlerinde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır. Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır.
    - Hasta kendi verisine online olarak hiçbir zaman erişmemelidir.
    - Bir Aile hekimi ancak kendisine kayıtlı olan hastaların elektronik sağlık kayıtlarına erişebilmelidir.
    - Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde ve ancak hasta kendisi ile ilgili sağlık kayıtlarının erişimine yazılı olarak onay vermiş ise hastanın elektronik sağlık kayıtlarına erişebilirler. Ve bu da “geçici bir süreliğine” olacaktır.
- Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetimi özellikleri kullanılacaktır.
- Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.
- Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin

verilmemelidir.

- Eğer hasta, herhangi bir sağlık çalışanının elektronik sağlık kayıtlarına erişmesini istemiyorsa,sağlık çalışanı ilgili dosyayı okuma hakkına kavuşamamalıdır. Fakat sağlık çalışanı muayene sonuçlarını hastanın veri tabanına aktarabilmelidir. Bu diğer doktorlar tarafından yazılan kayıtlara erişilmemesi için kullanılan metottur.
- Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.
- Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
- Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.
- Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.
- Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb token cihazları kullanılmalıdır.

- Sertifika tabanlı kimlik doğrulama yapılmadığı halde password ve hash tabanlı kimlik doğrulama yapılacaktır. Sistemlere erişim için tek yönlü şifreleme algoritmaları kullanılacaktır.
- Kurum içerisinde veya Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır. Bütün iletişim VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır.

APPENDIX C: CODE SAMPLES

Simplified code of SuperField class:

```
package ehr;
public class SuperField extends SuperRecord{

   /// Integer field
   protected int intF = 0;
   /// String field
   protected String stringF = "";
   boolean multiLine = false;
   /// hash table field
   protected Map mapF = new HashMap();
   /// vector field
   protected Vector vectorF = new Vector();
   ///dateCollection field
   protected Date dateF =null;
   //booealn field
   protected boolean booelanF = true;
   //float field
   protected float floatF = 0;
   protected String type = "" ;

   /// Constructor to set the fieldId
   private SuperField(EntityId entityId, String labelString, String labelId) {
      this.entityId = entityId;
      this.borderString = labelString;
      this.labelId = labelId;
   }

   /// Constructor to set the fieldId and integer field value
   public SuperField(EntityId entityId, int intF, String labelString, String labelId) {
      this(entityId, labelString, labelId);
      this.intF = intF;
      this.type = "2";
   }

   /// Constructor to set the fieldId and String field value
   public SuperField(EntityId entityId, String stringF, boolean multiLine, String
labelString, String labelId) {
      this(entityId, labelString, labelId);
      this.stringF = stringF;
      type = "1";
      this.multiLine =multiLine;
   }

   /// Constructor to set the fieldId and hash table field value
   public SuperField(EntityId entityId, Map mapF, String labelString, String labelId)
{
      this(entityId, labelString, labelId);
      this.mapF = mapF;
      type = "7";
   }
```

```
    /// Constructor to set the fieldId and vector field value
    public SuperField(EntityId entityId, Vector vectorF, String labelString, String
labelId) {
        this(entityId, labelString, labelId);
        this.vectorF = vectorF;
        type = "6";
    }

    /// Constructor to set the fieldId and boolean field value
    public SuperField(EntityId entityId, boolean booleanF, String labelString, String
labelId){
        this(entityId, labelString, labelId);
        this.booelanF = booleanF;
        type = "4";
    }

    /// Constructor to set the fieldId and float field value
    public SuperField(EntityId entityId, float floatF, String labelString, String
labelId){
        this(entityId, labelString, labelId);
        this.floatF = floatF;
        type = "5";
    }

    /// Constructor to set the fieldId and Date field value
    public SuperField(EntityId entityId, Date dateF, String labelString, String
labelId){
        this(entityId, labelString, labelId);
        this.dateF = dateF;
        type = "3";

    }
}
```

The code to transfer a simple class label to full confidentiality class name:

```
 public int getVectorElementIndex(String classIndicator) {

        int j = -1;

        for (int i = 0; i < classLabelVector.size(); i++) {
            if (((ClassLabel)
classLabelVector.elementAt(i)).labelId.equalsIgnoreCase(classIndicator)) {

                j = i;
                break;
            }

        }
        return j;
    }
```

An XACML policy for "GP" role, "Personal Identifiable" confidentiality class, and "view" and "change" actions:

```
<Policy PolicyId="100-00-00_01-00"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:ordered-permit-overrides">
```

<Description>
This policy applies to Role GP with role Id = 100-00-00 accessing 01-00-Personal-Identifiable classification level objects with classification/labeling Id = 01-00 . Final fall-through rule that returns Deny.
</Description>
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">100-00-00</AttributeValue>
<SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
</SubjectMatch>
</Subject>
</Subjects>
<Resources>
<AnyResource/>
</Resources>
<Actions>
<AnyAction/>
</Actions>
</Target>
<Rule RuleId="01-00-Personal-Identifiable" Effect="Permit">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">01-00-Personal-Identifiable</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">view</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="01-00-Personal-Identifiable" Effect="Deny">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>

```
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">01-
00-Personal-Identifiable</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">change</AttributeValue
>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

Sample policy for a “Nurse” role and access rights for “Public” confidentiality class”:

```
<Policy PolicyId="500-10-00_03-00"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:ordered-permit-overrides">
<Description>
This policy applies to Role Nurse with role Id = 500-10-00 accessing 03-00-Public
classification level objects with classification/labeling Id = 03-00 . Final fall-through
rule that returns Deny.
</Description>
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">500-
10-00</AttributeValue>
<SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</SubjectMatch>
</Subject>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">03-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
```

```
</Resource>
</Resources>
<Actions>
<AnyAction/>
</Actions>
</Target>
<Rule RuleId="03-00-Public" Effect="Permit">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">03-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">view</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="03-00-Public" Effect="Permit">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">03-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">change</AttributeValue
>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

```
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="03-00-Public" Effect="Deny">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">03-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

Sample policy for a “Nurse” role and access rights for “Public” confidentiality class”:

```
<Policy PolicyId="500-10-00_06-00"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:ordered-permit-overrides">
<Description>
This policy applies to Role Nurse with role Id = 500-10-00 accessing 06-00-
Confidential classification level objects with classification/labeling Id = 06-00 .
Final fall-through rule that returns Deny.
</Description>
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">500-
10-00</AttributeValue>
<SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</SubjectMatch>
</Subject>
```

```
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">06-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<AnyAction/>
</Actions>
</Target>
<Rule RuleId="06-00-Confidential" Effect="Permit">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">06-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">view</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="06-00-Confidential" Effect="Deny">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">06-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
```

```
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">change</AttributeValue
>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="06-00-Confidential" Effect="Deny">
<Target>
<Subjects>
<AnySubject/>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">06-
00</AttributeValue>
<ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</AttributeValue>
<ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
<Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```