A Negotiation-based Approach to Resolve Conflicting Privacy Policies in M-Health

Souad SADKI[1], Hanan EL BAKKALI[2]
[1,2] Laboratory of Information Security Research Team (ISeRT)
National Higher School of Information and Systems Analysis
Mohammed V University, Rabat, MOROCCO
souad.sadki@um5s.net.ma, h.elbakkali@um5s.net.ma

ABSTRACT: *Recently, there has been a growing interest in the usage of mobile services and applications for healthcare. However, this growth also brings on many challenges such as privacy preservation. Many research works have been carried out emphasizing the important role privacy policies play in protecting patients' private data from any kind of violation or misuse. In fact, policies are expressed using natural languages reflecting different actions third parties may perform on patient's data. These policies may not necessary satisfy patients' privacy preferences leading to conflicting situations. In this paper, we compare some privacy policies languages suggested in the literature taking into account a number of criteria such as high-expressiveness, abstraction and delegation of authority support. Also, we propose an approach aiming at resolving conflicts among privacy policies by negotiation. Finally, in order to show how our solution can be applied, we consider an example of conflicting privacy policies. For that, we adopt S4P, a language for specifying both patients' preferences and third parties' policies and which satisfy the different criteria considered in the comparative study.*

Keywords: Mobile Healthcare, Privacy Policy Language, S4P, Conflicting Policies, Negotiation

Received: 29 May 2015, Revised 3 July 2015, Accepted 10 July 2015

1. Introduction

Mobile health (mhealth) has recently grown a lot of attention as it plays a crucial role in improving patients' quality of care and reducing related costs. Indeed, mobile health technologies and applications allow individuals to more efficiently and easily self diagnosis their symptoms, enabling their "digital" engagement in their care. Furthermore, it enhances tracking, monitoring and communicating medical information such as blood pressure, oxygen saturation or glucose levels especially for patients with chronic diseases [22]. According to the findings from the 5th Annual Makovsky/Kelton "Pulse of Online Health" Survey, almost two-thirds (66%) of Americans would use a mobile application to manage health-related issues in the near future [24]. A prominent example that emphasizes the important role mobile technologies play is when a cardiologist saved a passenger's life when he diagnosed his critical heart disease on the plane using a wireless device attached to his phone [20].

Nevertheless, mobile technologies used for healthcare raise tremendous concerns including privacy leakage. In fact, privacy is a fundamental concept that should be properly addressed. In effect, mobile devices collect different sort of data (medical and no

medical) from different sources. This data is most of time unregulated which increases patients' fear over the privacy of their sensitive information. Particularly, with the emergence of Cloud-based services for healthcare, it becomes even harder to ensure user privacy with the multiplicity of the involved parties in patients' care.

In order to protect patients' data from possible misuse or unauthorized disclosure, privacy policies for mobile applications are needed. These policies are considered as a basis allowing users to decide whether or not to disclose their sensitive information [5]. So, the challenge is on defining human-readable privacy policies, understandable and that can be easily translated into language machine.

Previous researches have emphasized the important role privacy policies play in protecting users' data. For that, many privacy languages such as P3P [6], XACML [10] and EPAL [11] have been developed. However, most of these languages fail to respond to patient's needs in terms of specifying their privacy preferences and matching them against policies [5]. Also, the majority of these languages have a fixed vocabulary which limits their expressiveness. Finally, the heterogeneity of these policies (diversity of domains of application, diversified vocabularies and requirements, different level of abstraction [5]) leads to several problems such as conflicting policies.

To tackle this issue, we propose an approach based on a negotiation mechanism. This solution is an extension of our previous work defined in [21]. In fact, we believe that the patient is a particular user. He has the right to express his privacy preferences and be informed of every "move" that third parties may take regarding the usage and the divulgation of his sensitive data. Thus, efforts have been made to make it as simple as possible for patients to express their privacy preferences and to be involved in any decision or action regarding the safety of their data.

The paper is organized as follows. In Section 2 we compare some privacy policy languages suggested in the literature taking into account a number of criteria including high expressiveness and delegation of authority support. Section 3 presents our approach. In Section 4 we present an example of conflicting privacy policies where we show how our approach can resolve the conflict in question. In Section 5 we present some research works carried out in relation with privacy policies and negotiation mechanism. Section 6 concludes the paper and introduces some future works.

2. Privacy languages: Comparison and Related Issues

Patients are becoming more and more aware of privacy concerns. Thus, they want to be able to express their privacy preferences and disclose their data to trustful parties or other parties that satisfy these preferences [9]. For this end, privacy policies were made to describe how users' data is used, to which parties this data is divulgated and for what purposes. But, these policies must simultaneously reflect the wishes of users and service providers.

In the m-health sector, most existing privacy policies for mobile heath systems require a high-level literacy, do not make information privacy practices transparent to costumers, and are in mostly not focused on the mobile application itself. [16]. Moreover, even if the majority of users are concerned about their privacy, they usually avoid reading privacy policies [5]. According to a study performed by Drs. Sunyaev and Mandl , most of privacy policies that exist in 30.5% of the most popular mHealth applications on the market are long and hard to read [16]. Furthermore, privacy rules contained in these policies need to go through a formalization process to generate formal privacy policies from a regulatory text [8].

Moreover, and since patients are more and more integrated in managing their health, they now have the ability to efficiently access and share medical information and receive the care they deserve whenever they are. But, in order to assure data privacy, the sharing of these data must be regulated [2].

In this paper, we focus on privacy policies formalization and conflicting privacy policies resolution. The challenge is on defining a formal and flexible language that is human-readable, easy to understand and to be transformed into language machine. However, every actor defines its privacy policies (preferences for patients). The problem is that policies are highly heterogeneous, they are proliferated horizontally (different application domains with varying vocabulary and requirements) and vertically (expressed across all abstraction layers) [5]. As a result, conflicts among these policies may take place. In order to resolve this kind of conflicts, negotiating privacy policies to reach an agreement between the opponents parties remain the most appropriate solution particularly in healthcare where patient's safety matters more than anything else.

Criteria / Privacy Language	Abstraction	Satisfaction between User Preferences and Service Policies?	Distinguish between Permissions and Promises	Human-readability	High-Expressiveness	DA support	Score
P3P (Platform for Privacy Preferences) [6]	-	-	-	-	-	-	0/6
XACML (eXtensible Access Control Markup Language) [10]	-	-	-	+	+	+	3/6
EPAL (Enterprise Privacy Authorization Language) [11]	-	-	-	+	+	-	2/6
DPAL (Declarative Privacy Authorization Language [27]	-	-	-	-	-	-	0/6
PRML (Privacy Rights Markup Language)[14]	+	-	-	-	+	-	2/6
PERFORM (PERvasive FORmal Privacy Language) [15]	-	-	-	+	+	-	2/6
P2U (Purpose-to-Use) [4]	-	-	+	+	-	-	2/6
CPL (Consumer Privacy Language) [7]	+	-	-	-	+	-	2/6
SIMPL (Simple privacy language) [6]	-	+	+	+	-	-	3/6
S4P [5]	+	+	+	+	+	+	6/6

Table1. Comparison of some privacy policies according the design goals defined in [5]

2.1 A Comparative Study

Taking into account the aforementioned privacy policies concerns, we compare in Table 1 some privacy policies languages that have been proposed in the literature. The comparison is based on the six design goal defined in [5]. Some privacy languages presented in the literature are compared based on these goals. According to [5], the six criteria that should be satisfied in a privacy language are described as follows:

• **Human-Readability:** Since privacy policies are highly heterogeneous [5], it is crucial to make these policies as simple as possible in order to be understood by different actors.

• **High-Expressiveness:** A high degree of expressiveness is required in a privacy policy. In fact, a privacy language can be manipulated by heterogeneous actors and with a variety of application domains.

• **Abstraction:** It refers to the ability of a privacy language to hide the semantics of service behaviors using abstraction representation in order to support a vast range of policies [5].

• **Distinction between Preferences and Policies:** We believe that patients have the right to express their privacy preferences over their sensitive information usage and disclosure. Thus their privacy preferences have to be distinguished from third parties' policies. Here, distinction concerns permissions and promises [5].

• **Satisfaction between User Preferences and Service Policies**: This is criteria determines whether a mechanism to verify services policies satisfaction over users' data exists or not.

• **Delegation of Authority (DA) Support:** Here, we verify if the language permit the delegation of authorities to other trusted parties.

As indicated in Table 1, the privacy language satisfying the five designed goals is S4P; a formal language that machine can interpret [5]. S4P distinguishes between privacy policies which refers to third parties and privacy preference that concerns the costumer.

Furthermore, S4P language is highly expressive, easy to read (human-readability characteristic) and flexible thanks to the abstraction characteristic.

Moreover, assigning a part of responsibility to entrusted parties in need is crucial especially in urgent situations when patient life become a priority. For these reasons, we will use S4P in the rest of the paper to express both patients' preferences and third parties' policies

2.2 Overview of S4P language

As described in the previous section, S4P distinguishes between services policies and customers preferences and allows the satisfaction checking between the two [5]. Policies and preferences in S4P are presented in a form of assertions and queries [5].

An *assertion* is Defined as: < *E* ***says*** f_0 ***if*** $f_1 \ldots f_n$ where c >; where E defines a user or a third party, the fi are facts and c is a constraint on variables occurring in the assertion [5].

We suppose E is a Healthcare Provider (HP), P is a patient, PII for Personally Identifiable Information.

Example of an assertion:

Bob **says** *x* **may** use PII ***if*** *x* will revoke PII within *t*

E f_0 f_1

where *t* < 1 year ^ x = {medical organizations}

C

According to [5], an S4P query *q* is defined as follows:

q:: == E **says** f? | c? | ¬q | $q_1 \wedge q_2$ | $q_1 \vee q_2$ | $\exists x\,(q)$

Examples of S4P queries:

• E **says** f? :

P **says** *HP* **may** share PHI with other healthcare providers**?**

• q1 ^ q2:

HP **says** HP **will** use PHI for treatment? ^ HP **says** HP **will** use PHI for research purposes?

a) Preferences in S4P
Assertions in a preference or **May-assertions** express what a service (third party) *may*, or is permitted to do with the user's (patient in our case) sensitive information [5].

Query in a preference or **will-query** expresses obligations, i.e. the behaviors that third parties *must* exhibit [5].

b) Policies in S4P
Assertions in a policy or **will-assertions** describes what a service *will* certainly do, or promises to do with users data [5].

Query in a policy or **may-query** expresses and advertises all possible relevant behaviors of the service [5].

	User preferences	**Service Policy**
Permissions	may-assertions **User gives permissions**	may-query **Service asks for permissions**
Promises	will-query **User asks for promises**	will-assertions **Service gives promises**

Table 2. Assertations And Queries In S4p[5]

In order to provide efficient care for patients, assigning a part of the authority to others parties is sometimes required or even mandatory especially in urgent situations. Thus, language describing privacy policies and preferences has to support delegation of authority. In S4P, the modal "can" is used to express delegation of authority.

Example:

Bob **says** HP **can** use PII if HP complies with HIPAA.

3. Description of the Proposed Approach

In this section we describe our negotiation-based approach for resolving conflicts among privacy policies/preferences. Precisely, we adopt the S4P language to express both patients' preferences and service providers' policies. In fact, our work extends our previous privacy preserving approach for m-health (PPAMH) [17] aiming at maximizing patients' control over their data in mobile health environments. Based on the bargaining model [19], a framework and an algorithm for solving security policies conflicts were suggested in [1]. We get inspired by this solution to define an approach to resolve the issue of conflicting privacy policies in mobile health environments based on the negotiation concept. We aim to preserve patient's privacy whether he is involved in the negotiation process or not. More importantly, we add the "intelligence" concept in our solution to make it as simple as possible for patients to express their privacy preferences regarding any action concerning their sensitive data, and to facilitate the conflict resolution on the other hand.

3.1 Policies/preferences formalization process
In order to facilitate the detection of conflicting policies, the first step is to formulize these policies, usually expressed using natural languages, in a formal way. For this purpose, we adopt S4P language which is particular from other privacy languages (cf. Section 2) and that distinguishes between user privacy preferences and service providers' policies.

Particularly, since patients are "special users", we believe that they should be involved in every decision regarding the operations related to their sensitive medical information. This data have to be protected whatever the condition of the patient is. From this perspective, as indicated in Table 2, we classify patients into four main groups [17, 18]: The Fundamentalist, the Pragmatic, the Unconcerned and the Should-Be-Protected group [17, 18].

Privacy Group	Description	Assigned level
Fundaentalist	Patients that distrust third parties to protect their privacy [17,18].	PL1
Pragmatic	Patients who prefer to decide whether they should trust organizations or ask for legal procedures to protect their personal information [17,18]	PL2
Unconcerned	Patients that trust health organizations or any third party to protect their private data [17,18].	PL3
Should-be-protected	Patients whom health condition does not allow them to make preferences. This group includes children that can't take proper decision and need a guardian or patient badly hurt [17,18].	PL3

Table 3. Patients' Privacy Groups And The Assigned Levels [17]

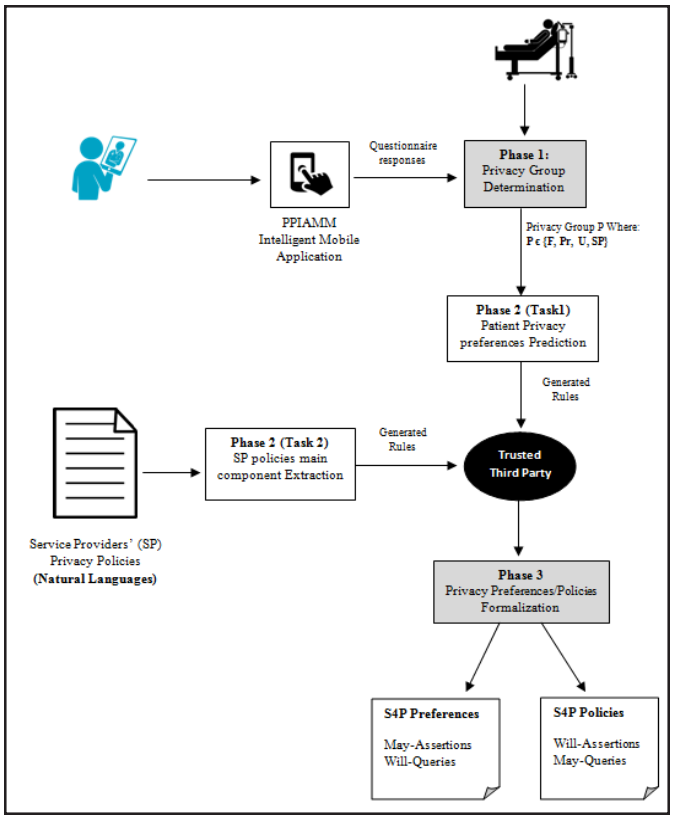

Figure 1. Privacy policies/preferences formalization process

This group serves as an indicator for deducting patients' privacy preferences according to his behaviors (Phase 1). That said, Patient's privacy preferences are predicted using an intelligent mobile application that "deducts" patients' preferences based on a questionnaire that they should answer [17]. Table 2 describes the particularity of each group as well as the privacy level associated to each group facilitating this way the preferences prediction operation.

As shown in Figure 1, after patients' privacy preferences are predicted according to the privacy group to which the patient belongs (Phase 2). A set of rules is generated and send to a Trusted Third Party allowing privacy preferences/policies expression in a formal way using S4P language (Phase 3).

3.2 Main Components

In this section, we present the main entities involved in our solution. Precisely, we consider:

(1) **The Patient (*mp*)**: A Patient with a mobile device (Smartphone or Tablet). A patient *mp* can be a Fundamentalist (F), An Unconcerned (U), a Pragmatic (P) or a Should-Be-Protected (SP) patient [21].

(2) **A Service Provider (*SP*)**: A Healthcare Provider or a Cloud Provider.

(3) **Trusted Third Party (*TTP*):** it plays an intermediary role between patients and third parties. First, it is responsible for transmitting negotiation requests to patients. Second**,** it also informs the service providers of the patient privacy group to facilitate the negotiation process. Also, it plays the role of the negotiator in case the patient belongs to the "Unconcerned" or the "Should-be-Protected" group.

Obviously, it's quite difficult to negotiate with a fundamentalist patient than negotiating with a pragmatic patient. (The fundamentalist patient needs more arguments and efforts). For this reason, we define three level of negotiation:

- ***NL1*** (Negotiation level 1): Patient who needs strong arguments and efforts to agree to negotiation (The Fundamentalists)

- ***NL2*** (Negotiation level 2): Patient who can easily accept negotiation if they understand and accept the purpose or constraint for which a third party want to negotiate an accurate policy.

- ***NL3*** (Negotiation level 3): Default level where the trusted third party, which is responsible for protecting patient's privacy, relies on *the purpose of usage* to negotiate the conflicting privacy policies.

3.3 Conflict Detection

In this work, we assume patients' privacy preferences and services providers' policies are written in S4P language. As described in the previous section, S4P preferences/policies are formed of *assertions* and *queries*.

Obviously, a conflict between a preference and a policy means that this policy doesn't satisfy patient's privacy preference.

According to [5], Checking that a policy satisfies a preference consists of two steps.

- Every behavior declared as *possible* in the policy must be *permitted* by the preference.

- Every behavior declared as *obligatory* in the preference must be *promised* by the policy.

In other words, the May-queries and Will-queries must be satisfied as indicated in the following relation [5]:

(1) $A_{pl} \cup A_{pr} - q_m \wedge q_w$

Where A_{pl}, A_{pr}, q_m and q_w respectively designate a set of assertions in patient's privacy preferences, a set of assertions in service provider privacy policies, patient' will-queries and service' may queries.

3.4 Negotiation Steps

Our negotiation approach for solving conflicts among privacy policies is based on the work defined in [1]. Authors in [1] propose a framework and an algorithm to negotiate security policies. It consists of four stages: Information stage, Demand stage, Bargaining stage and Contract establishment [1].

As illustrated in Figure 2, there are five main stages in our negotiation process:

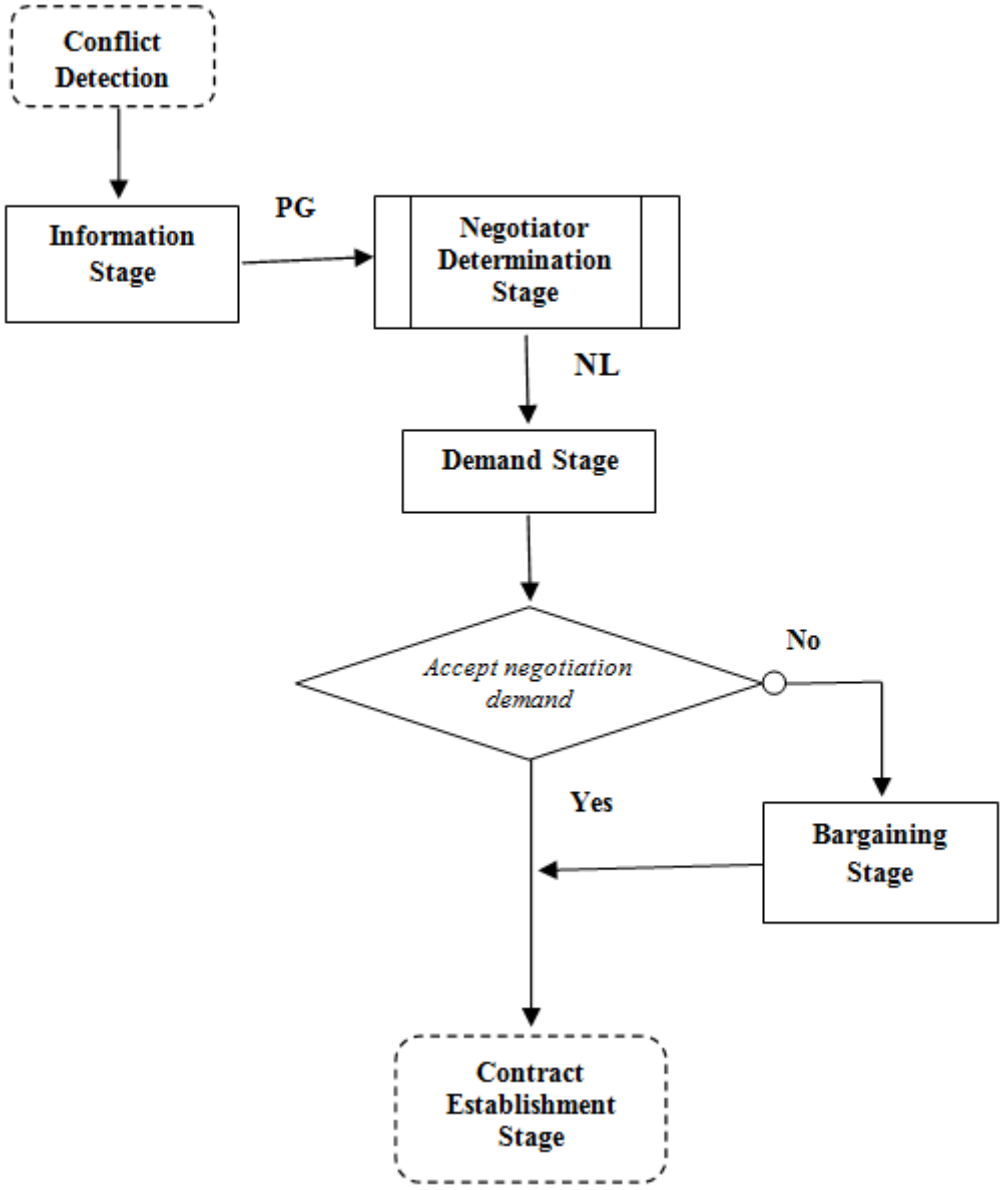

Figure 2. Negotiation stages

3.4.1 Information stage

In this stage *TTP* inform the *SP* whose privacy policy is conflicting with *mp* preferences about the patient's privacy group. This operation allows SP to have a previous knowledge about patients' behavior when a negotiation session starts. SP can hence "expect" patient's response over negotiation demands.

3.4.2 Negotiator determination algorithm

Patient privacy preferences are predicted according to privacy group which does not only facilitates patients' policies generation

but also determinates the level of negotiation that should be assigned to the patient. If a conflicting situation occurs between patients' preferences and a third party privacy policy, TTP starts by defining if the patient can be involved in the negotiation process (algorithm 1). F or the "Unconcerned" category, it can be changed to "Fundamentalist" or "Pragmatic" when the patient becomes aware of the different risks that can endanger his privacy when using a mobile device [21]. For this reason, PPIAMH was designed with the privacy awareness functionality where the patient is asked to answer a list of questions (*score*) [21]. If the patient becomes concerned the function **CalculNG (score)** is applied indicating the new privacy group.

3.4.3 Demand Stage

After specifying the level of negotiation, TTP sends the third party's negotiation request (demand stage) to the patient (if he is involved in the negotiation process). If the patient accepts the opponent's offer a "CreateAgreement" message is created. Otherwise, the two participants enter the bargaining stage where a final decision must be made (accept, refuse).

Algorithm 1: Negotiator determination group

Input : privacy group type **Pg** where **G ∈ {F; P; U; SP} Output**: **N //** Negotiator

1. We define the following Boolean variable:

Aw: set to 1 if the awareness functionality is active

// Conflict detection if (¬ (Apl ∪ Apr ⊢ qm ^ qw))

2. **//** Negotiator determination stage

3. **if (Pg** = "F" || **Pg** = "Pr"**)then**

4. **N ← mp; // The patient is the negotiator**

5. **else**

6. **if (Pg** = "U"**) then**

7. **// We activate the awareness functionality**

8. **A*w* ← 1;**

9. **NG = CalculNG(Pg); //** Calcul the new group

10. **if (**NG!= **Pg)**

11. **N ←** *mp;*

12. **else**

13. **N ←** *TTP;* TTP is the negotiator

14. **endif**

15. **endif**

16. **N ←** *TTP;* // **U** = "SP"

17. Return N

18. **endif**

19. **endif**

20. End

3.4.4 The Bargaining Stage

In the bargaining stage, the third party relies on the negotiation level to negotiate the privacy policy with the patient. That said,

the policy can be changed (or temporary changed) if the patient (if he is the negotiator) is convinced of the arguments (purposes of usage) given by the opponent party or if access to data is mandatory (urgent situations).

To illustrate this point, we consider the example of a Pragmatic patient who uses a mobile application to access his personal health record and interact with his doctors. The patient's privacy policy indicates that he restricts access to his data to his local physicians and family members only. However, the pragmatic patient policy can be changed based on the arguments: "you can save a life by sharing your medical experiences with patients (especially children)" where he can allow the sharing of his data with patients having the same disease via a health social network for instance.

3.4.5 Contract Establishment Stage

After the negotiation process is done. A contract between the patient and third parties has to be established. TTP is responsible for establishing this contract. It is considered as a proof of the negotiation result. Also, it allows the trusted third party to "expect" the patient decision when a similar situation (conflict) takes place.

4. Conflict Scenario

In this section, we present an example of conflicting privacy policies/preferences expressed using S4P. The following notations are used: ***TP*** for third parties, ***HP*** referring to Healthcare providers.

We consider the example of a healthcare provider; Arkansas Children's Hospital (ACH) [25], a pediatric medical center in the United States. We also consider a Cloud Provider (CP), CloudHealth technologies [26] which provides different services to healthcare providers and other enterprises. Each of ACH and CloudHealth possesses a privacy policy describing how customers' data is handled and shared.

Bob, 16 years old, is a patient at ACH hospital. Since Bob is minor, all the operations and decisions related to his health are taken by his mother (guardian), Alice who uses "MyACH" mobile application [25] to access her child medical history, get information about health symptoms and get an appointment. Bob's mother is very concerned about the privacy of her son's sensitive data, in particular, his personally identifiable information.

4.1 Preferences/Policies Description

S4P is used to express Bob's privacy preferences (defined by his guardian) as well as ACH and CloudHealth privacy policies. We assume a part of Alice's privacy preferences regarding her son's data usage and disclosure are defined as follows:

• Bob Preferences (Defined by his guardian)

May-Assertions:

(1) Alice says *HP* **may** *use* PHI for treatment purposes only.

(2) Alice says *HP* **may** *share* Medical Data where $x \in$ {Healthcare Organizations, Government Authorities}

Will-Query:

(3) HP says HP **will** retain PHI for t where $t < 2$ years

(4) ACH says ACH **will** share PHI for *purp* where $purp \notin$ " {Auditing, advertizing}**?**

In the may-assertion (1) Alice requires any healthcare provider to use her son's data for medical purposes only whereas in the may-assertion (2) she allows *HPs* to share this data with other healthcare organizations or government authorities only. In the will-query (3), Alice requires service to not retain her PHI for more than two years. In the will-query (4), Alice requires ACH not to use Bob's PHI for auditing or advertizing.

• ACH policy

The following statements are taken verbatim from ACH Online Privacy policy [25]

"*Your PHI may be used for research purposes in certain circumstances with your permission"*

"*We may share some of your PHI with outside people or companies who provide services for us"*

"We must disclose your PHI to government authorities that are authorized by law to receive reports of suspected child abuse or neglect involving children or endangered adults"

The three above privacy policies can be expressed in S4P as follows:

Will-Assertion
(5) ACH **says** ACH **will** *share* your PHI with *TP* for *purp* if
TP is a government agency where *purp* ϵ {child abuse, neglected children, endangered adults}.

May-Queries
(6) ACH **says** ACH **may** *use* PHI for research purposes**?**
(7) Alice **says** ACH **may** *share* PHI with outside services**?**

The will-assertion (4) indicates that ACH hospital can share some of patients' PHI with government agencies in order to prevent child abuse, neglected children or endangered adults. In the may-queries (5) and (6), ACH asks for permission to use user PHI for research purposes and to share this data with external parties that can provide services for ACH hospital.

• CloudHealth Technologies Policy

We consider the example of a CP, CloudHealth technologies, which furnish prominent services for healthcare. The following statements are taken verbatim from CloudHealth technologies policy [26].

"We only store data about you for as long as it's reasonably required to fulfill the purposes under which it was first provided by you unless a longer retention period is required or permitted by law".

"We may also use personal information for internal purposes such as auditing, data analysis and research to improve our products'.

Using S4P, we can express the above policies as follows:

Will-Assertion
(8) CloudHealth **says** CloudHealth **will** store personal information for t where t is *undetermined.*

May-Query
(9) CloudHealth **says** CloudHealth **may** use data *for auditing, data analysis and research purposes***?**

As described in CloudHealth online policy and the will-assertion (7), the duration of data storage is not specified. In fact, data can be retained for a long duration if the law imposes it.

In the may-query (8), CloudHealth asks for permission to use patient's information for auditing, data analysis or research purposes.

4.2 Conflicts Description

In this section we describe the conflict among Bob privacy preferences, ACH and CloudHealth privacy policies.

As indicated in the previous section, we say that a conflict between user's privacy preference and a service privacy policy takes place if this privacy policy *doesn't satisfy a* user preference. In other words, patients privacy preferences are not satisfied if the may-queries and will queries are not satisfied.

In Bob's may-assertion (1), his guardian allows any *HP* to use his PHI for treatment purposes only. For instance, the usage of this data is permitted if it is needed by another entity to improve patient's care. However, in ACH may-query (6), ACH asks for permission to use patients' data for research purpose which is different from the purpose imposed by Alice. But, this preference can be changed if the patient is aware of the importance of data usage for research reasons. Thus, integrating the patient in the decision-making is an important step towards protecting his privacy and improving his health and outcomes. The same goes with the may-assertion (2) where Alice restricts the sharing of Bob's data to healthcare organizations and government authorities only. But, ACH may-query (7) indicates that user information can be divulgated to other entities that provide other services for the hospital. For instance, we suppose that a CP such as CloudHealth technologies provide services (storage for instance) for ACH.

In the may-query (9) CloudHealth asks for permission to use patients' data for auditing, data analysis and research purpose which does not satisfy Bob may-assertion (1).

Tab.3 presents the *unsatisfied* may-queries and will-queries against May-queries and the will-query.

Remarkably, the conflict is not necessarily produced by the entity directly involved in patient's care. That said, other parties providing services for this entity can become the source of the conflict. For instance, we take the example of the will-assertion (5) where ACH promises to disclose user PHI to government authorities that are authorized by law to prevent child abuse, neglected children or endangered adults. This assertion satisfies Bob will-query (4) which indicates the purpose under which user data shouldn't be disclosed (which are different from the purposes presented in the will assertion (5)). Notably, government authorities are authorized to use Bob's data as shown in the may-assertion (1). Here, the conflict is provided by CloudHealth (indirect entity involved in patient care). Example of such conflict concerns the duration of data retention (will-assertion (8)) which does not satisfy Bob will-query (3) requiring services to store data for duration less than two years.

Will -Query	**Corresponding Will-Assertion**	**May-query**	**Corresponding May- assertion**
(3)	(8)	(6)	(1)
-	-	(7)	(2)
-	-	(9)	(1)

Table 4. Unsatified May-assertations And Will-query

Therefore, with the huge number of applications and actors involved in patients' care, ensuring privacy becomes even harder. Hence, the challenge is on finding a balance between third parties (services) goals and patients' privacy needs. For that, we believe that negotiation is among the best techniques to resolve the issue of conflicting privacy preferences/policies. Also, since patients are special customers, it is crucial to make it as simple as possible for them to negotiate their privacy preferences and take the adequate measures in their behalf when needed.

4.3 Application of Our Approach to Resolve the Conflict

Before resolving the conflict, the first step is to determine patients privacy group based on the intelligent application that predict patients preferences based on his answers to the questionnaire. In our case since the concerned patient, Bob, is a minor, there are two possibilities, whether he is classified as a "Should-Be-Protected" patient if there isn't any person to decide in his behalf. Or a guardian is involved in his care taking any action regarding the health operations and data privacy.

In our case, Alice answers a questionnaire; an example of question can be for instance:

Do you usually share your personal information with organizations that ask for it? Would you say you do this never, rarely, sometimes, often or always? [23]

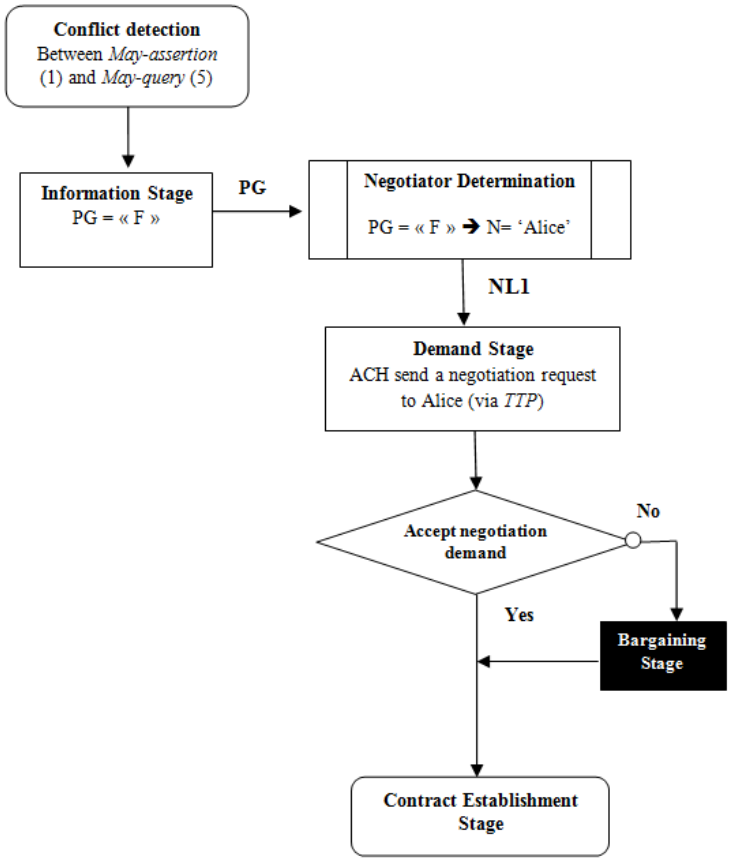

Figure 3. Negotiation stages to resolve the conflcit among the may-assertion (1) and the may-query (5)

We assume that she is classified as a Fundamentalist. (She refuses any disclosure of her son's data with other parties).

We consider the may-assertion (1) against the may-query (5). As indicated in Figure 3, the first step consists on determining the privacy group as well as the involved parties in the conflict (Information stage). Next, the privacy group is taken allowing the determination of the negotiator (Negotiator termination stage). Then, before sending the negotiation demand, the negotiation level (deducted from the privacy group) is considered allowing the demander to have a previous knowledge about the opponent party. The negotiation demand is hence sent to Bob's guardian. In fact, there are two possibilities: whether Alice accepts ACH demand to share information for research purpose, in this case a contract is settled and sent to the trusted third party. Or, she refuses ACH offer and then the two parties enter the bargaining stage where ACH tries to find arguments such as: "by allowing us to use your data for research you can help your country overcoming several sorts of disease and save patients like you" to convince Bob's guardian. In this case, the negotiator (Alice) can accept the offer or remain fundamentalist. In the two cases, the contract between the two parties is established.

5. Related Works

Several privacy policies have been suggested in the literature. However, the majority of these languages do not distinguishes between policies that reflects third parties behaviors from policies that express users' privacy preferences and do not allow the satisfaction checking between the two [5] to detect and resolve any possible conflicting situation.

P3P [6] was created to present a website's privacy policy in a structured and machine readable way [3]. However, policies written

in P3P are very complex, opaque, and difficult to understand [1]. Also, user preferences cannot be expressed in P3P [5].

Additionally, languages such as XACML for access control do not satisfactorily deal with specifying user preferences and matching them against policies [5]. Consequently, generic privacy policy language such as S4P was defined trying to respond to these limitations.

Authors in [15] suggest a Pervasive Formal language called PERFORM. This language, which is quite similar to human level language, is characterized by defining policies in terms of "requests/responses" and "constraints." [15].In the same context, a privacy language; CPL (Consumer Privacy Language); was suggested in [7] reflecting user preferences in context-aware services. The proposed language focuses on consumer' privacy preferences and do not consider the possible interactions and possible conflicts with third parties' privacy polices expressed in different languages.

In order to provide flexibility and adaptability and avoid conflicts between policies, negotiation of some aspects of the policies is required. Unfortunately, most privacy languages lack negotiation mechanisms.

Some research works have considerate negotiation in the policy. Exemplary, we cite the language suggested in [4] where authors propose a privacy policy language called P2U (purpose-to-use) aiming to enforce privacy. It enables a secondary usage of information across applications, devices and services on the web [4]. Moreover, authors in [12] present an approach for negotiating privacy policies for an e-learning service. In this approach, negotiation is based on the usage of common interest and reputation mechanisms employing a list of parties that have negotiated the same problem in the past [12]. In the context of web services, authors propose a negotiation approach [13] to negotiate Service Level Agreements (SLAs). In particular, a trusted middleware and privacy policy specification were presented in order to facilitate and express the different parameter of negotiation [13].

We believe that negotiation is crucial in resolving conflicts among policies. It should be taken into account in any privacy language. Particularly in S4P, since detecting conflicts is simple and easy thanks to the distinction between preferences and policies, negotiation remain the best way to resolve the conflicting situations.

6. Conclusion

Based on a negotiation mechanism, we suggest an approach to resolve the issue of conflicting privacy policies in mobile healthcare environments. In particular, we adopt S4P as a privacy policy language formalizing both privacy policies/preferences. The classification of patients into four groups in term of privacy preferences facilitates the negotiation process since different levels of negotiation are suggested depending on the privacy group considered.

Based on this classification, a detailed algorithm describing the different stages of our solution will be developed. Besides, an extension of S4P language taking into account the defined privacy groups will be suggested.

References

[1] Yanhuang Li., Cuppens-Boulahia, N., Crom, J. M.,Cuppens, F., Frey, V. (2014). Reaching Agreement in Security Policy Negotiation. *In*: Proceedings of the IEEE 13th International Conference on Trust, *Security and Privacy in Computing and Communications*, 98 – 105.

[2] Lunardelli, A., Ilaria M., Matteucci, I., Paolo, M. (2013). A prototype for solving conflicts in XACML-based e-Health policies. *In*: Proceedings of the IEEE 26th International Symposium on Computer-Based Medical Systems . 449 – 452.

[3] Moritz, Y. Becker, A. Malkis, L. Bussard. (2010). A practical generic privacy language. *In:* Proceedings of the ACM 6th international conference on Information systems security, 125-139.

[4] Iyilade, J., Vassileva, J. 2014. P2U: A Privacy Policy Specification Language for Secondary Data Sharing and Usage, *In*: Proceedings of the IEEE Security and Privacy Workshops, 18-22.

[5] Moritz Y. B., Alexander M., Laurent B. (2010). S4P: A Generic Language for Specifying Privacy Preferences and Policies, Technical report MSR-TR-2010-32, Microsoft Research.

[6] Cranor, L., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M. Presler-Marshall, J., Reagle, M., Schunter, D. Stampley, A., Wenning R. (2006). The Platform for Privacy Preferences 1.1 (P3P1.1) Specication. W3C.

[7] Kapitsaki, G. M. (2013). Reflecting User Privacy Preferences in Context-Aware Web Services. *In:* Proceedings of the IEEE 20th International Conference on Web Services. 123 – 130

[8] Alshugran, T., Dichter, J. (2015) Rusu, A., *In*: Proceedings of the IEEE Systems, Applications and Technology Conference, 1-5.

[9] Moritz, Y., Becker Alexander, M., Laurent, B., (2009). A Framework for Privacy Preferences and Data-Handling Policies, Microsoft Research; technical report MSR–TR–2009–128.

[10] OASIS. (2005). eXtensible Access Control Markup Language (XACML) Version 2.0 Core specification.

[11] Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M. (2003). Enterprise Privacy Authorization Language (EPAL 1.2). Technical report, IBM, November.

[12] George Y., Larry K. (2003).The Negotiation of Privacy Policies in Distance Education. *In*: Proceedings of the 14th International Conference, Philadelphia, Pennsylvania.

[13] Zulkernine F., Patrick M., Craddock C., Wilson K. (2009). A Policy-based Middleware for Web Services SLA Negotiation. *In:* the proceedings of the IEEE International Conference on Web Services. 1043 – 1050.

[14] Zero knowledge.(2005), Privacy Rights Markup Language (PRML) Specification. Tech. rep., Oasis, Retrieve. http://www.synomos.com/html/EPML/documents/prmlspec.pdf. June 17.

[15] Dehghantanha, A., Udzir, N.I. ; Mahmod, R. (2010). Towards a Pervasive Formal Privacy Language. *In* Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops.1085 – 1091.

[16] Sunyaev, A., Dehling, T., Taylor, PL., Mandl, KD. (2014), availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association , 22 (1) e28-e33.

[17] Sadki, S., El Bakkali, H. (2014). PPAMH: A novel privacy-preserving approach for mobile healthcare. *In* Proceedings of the IEEE 9th International Conference for Internet Technology and Secured Transactions, 209 – 214.

[18] Westin A., Harris Louis Associates. (1991). Harris-equifax consumer privacy survey. Tech. Rep. conducted for Equifax Inc. 1, 255 adults of the U.S. public.

[19] Baida, R.E. , Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G. (2003). Organization based access control, *In*: Proceedings of IEEE 4th International Workshop in Policies for Distributed Systems and Networks. 120–131.

[20] Ronald, S., Weinstein., Ana Maria Lopez., Bellal A. Joseph., Kristine, A. Erps., Michael Holcomb., Gail P. Barker., Elizabeth, A. Krupinski. (2014) Telemedicine, Telehealth, and Mobile Health Applications That Work: Opportunities and Barriers .*The American Journal of Medicine*, 127 (3) 183–187.

[21] Sadki, S., El Bakkali, H. (2014). A Patient-Centric Approach for Intelligent Privacy Policies Generation in Mobile Healthcare. *International Journal of e-Healthcare Information Systems*. 1(1/2/3/4) 2-9.

[22] Steven, R., Evan, D., Eric, J., (2013), Can mobile health technologies transform health care? The Journal of the American Medical Association, 310 (22) 2395-2396.

[23] Phoenix strategic perspectives inc (SPI). (2013) Survey of Canadians on Privacy-Related Issues.

[24] Makovsky Health. (2015). Fifth Annual "Pulse of Online Health" Survey. January.

[25] Arkansas Children's Hospital. (2013). Joint Notice of Privacy Practices. http://www.archildrens.org/About-ACH/Privacy-Practices.aspx, revised August 29.

[26] CloudHeath technologies. Privacy policy. (2014). http://www.cloudhealthtech.com/privacy. January 21.

[27] Barth A., John Mitchell, J. C. & Rosenstein, J. (2004). Conflict and Combination in Privacy Policy Languages. *In:* Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society. 45-46. October 28.