# A Semantic Approach to Secure Electronic Patient Information Exchange in Distributed Environments

Atif Khan, Helen Chen, and Ian McKillop

David R. Cheriton School of Computer Science,
University of Waterloo
200 University Avenue West Waterloo, ON, Canada N2L 3G1
{a78khan,helen.chen,ian}@uwaterloo.ca

**Abstract.** Modern medical information systems collect large amounts of diverse patient data in order to facilitate a higher level patient care. Although desirable, this functionality has a tremendous potential for abuse, where patient information can be shared, disclosed and used for other (secondary) purposes. In most cases, patient consent is solicited and institutional policies are put in place to limit the privacy and security risks. However, in practice these measures have proven to be inadequate, resulting in violation of patient consent even for non-life threatening scenarios. We propose a framework to capture privacy & security policies and to protect exchange of sensitive medical patient information. Our framework is comprised of distributed multiagent environments reflecting healthcare institutions and personnel. We utilize semantic techniques for data representation and reasoning. Furthermore, we do not require pre-established trust relationships to be present for exchanging private sensitive information between multiple parties. In our proposed framework, all decisions to share information, are backed up by semantic proof of authorization that can be verified by an independent third party.

## 1 Introduction

Modern medical information systems, along with Information Communication Technologies (ICTs), are key enablers for providing patients with a high level of medical care [15]. These systems capture and process large amounts of heterogeneous data from many diverse and distributed sources. Furthermore, information can be exchanged between various parties in many different formats, ranging from summaries of medical records to detailed diagnoses and test results.

Although the use of above mentioned technologies drastically improves the effectiveness of information exchange, coordination, and use, it also raises the critical issue of patient information privacy and security. Usually, patient information is collected for the primary purpose of providing healthcare for a specific episode. Any secondary usage must be in accordance with and governed by patient consent. It has been argued that a patient should be aware of all the systems collecting their information, and should be able to specify how this information can be used [14]. Given the complexity and diversity of medical information exchange scenarios, patient consent and privacy policies are often ignored for the greater good.

The use and protection of sensitive patient medical records is further complicated by the fact that these records are fragmented over many distributed heterogeneous storage systems. Although the information contained in these distributed segments is to be used in accordance with a global patient consent policy, each individual medical information system may be governed by its own privacy and security policies. Furthermore, these privacy and security policies might be augmented by jurisdictional policies (such as a provincial healthcare privacy and security act).

In this paper, we present a framework for describing, capturing, processing and managing sensitive patient medical information, based on patient consent and other applicable privacy and security policies. Our solution is centralized around the observations that (a) information contained in a patient's medical record should be governed by the patient's consent policy and (b) the security and privacy of the physical/electronic medical records must be guaranteed by the institutional privacy and security policies. Our proposed solution strives to honour both of the above mentioned conditions.

In our proposed system, all knowledge representation, acquisition, and exchange is based on the use of ontologies best suited to describe the various information sets. For example, patient consent is obtained and represented based on any ontology capable of defining the concepts required to capture such information. The main motivation to use an ontological approach is (a) to facilitate the exchange of information with other parties and (b) to represent information in an automated machine processable format.

Given the diversity of healthcare professionals and the heterogeneity of medical information systems, along with the complexity of information exchange, we have chosen to represent the healthcare domain as a distributed multiagent system. In our multiagent environments, each intelligent agent either represents an entity or acts as a proxy to an entity. All entities exist in a cooperative mode working towards maximizing the overall system utility. The system utility is measured in terms of the total benefit provided to a patient as a result of agent interactions.

In order to ensure the privacy and security aspects of all information exchanged between agents, we define an *information exchange handshake protocol*. We make the assumption that all agents can be monitored within their respective environments and therefore are not capable of being malicious. The protocol starts with the *request for information* where an agent sends a request for accessing sensitive medical data from another agent. The second phase of the protocol deals with validation of the various policies guarding the sensitive information. The requesting agent is asked to fulfil the security and privacy criteria identified by the agent holding the information. The requesting agent generates a proof in fulfilment of the requested criteria. The proof has the unique property of being verifiable by any party capable of computing it. Upon the validation of this proof, the requested information is delivered in response to the original request.

It is worth noting that at no point does our framework assume a (pre-established) trust relationship to have existed between the two agents exchanging information prior to the exchange. Each request for information is independently verifiable. Therefore, we can establish dynamic trust on a per request basis. Furthermore, considering that the validation of the policies protecting the patient information are part of each request response cycle, changes to these policies take effect almost immediately. This dynamic enforcement of patient consent and institutional privacy & security policies represent a major improvement over the trust-based [2] and role-based-access [22] medical information exchange frameworks.

In order to provide motivation for our work, consider the following example. *Let us assume that a patient John is primarily treated by Dr. Smith at the Toronto General Hospital (TGH). During his vacation in Calgary, John was found unconscious and was admitted to Calgary General Hospital (CGH). John is now being treated by Dr. Jane who requires access to John's past medical history, in order to properly diagnose and treat John. Dr. Jane requests access to John's medical records from TGH. For the purpose of illustration, lets us further assume*

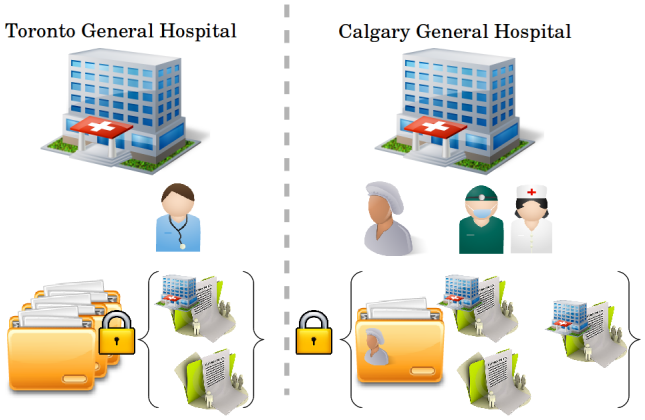


**Fig. 1.** A motivational example: John's EMR is protected by his consent and TGH's privacy & security policies. When Dr. Jane at CGH requests access to these documents, they are shared under the same protection that was offered by TGH. Furthermore, CGH may apply their own privacy and security policies in addition to the existing ones.

*that John's medical records are protected by his consent policy and the TGH institutional privacy and security policies*. Please refer to Fig:1.

The goal of our system is to allow Dr. Jane to be able to retrieve the required patient medical information (for John) from TGH, while still honouring all of the established privacy and security policies put in place by the institution and John's consent policy.

## 2 Related Work

Our proposed framework utilizes semantic knowledge representation and multiagent systems. Although both of these areas of artificial intelligence have been well researched and well understood, we have not found any existing work that utilizes semantic technologies with multiagent systems to address our goals specifically. In this section, we present a general literature review of these fundamental AI concepts. Our framework is motivated by the core concepts introduced and discussed in the papers selected in the literature review. The literature review focuses on semantic knowledge representation, various aspects of multiagent systems (such as use of semantic technologies in multiagent systems and trust establishment between agents) and electronic patient consent.

### 2.1 Traditional Authorization & Access Control

There have been several authorization and access control systems suggested in the literature [4,7,14,22]. Most of these systems are based on role-based access control (RBAC) and do not address patient consent. In RBAC, roles are associated with (access) privileges, and system users are then assigned roles based on the nature of their job or functionality.

Although the RBAC approach is quite effective within the confines of a single organization, it does not scale well when dealing with dynamic healthcare environments, where entities (such as doctors) can take on many different roles across many different organizations. Furthermore, RBAC based security frameworks are not real-time in nature. There is a considerable lag when it comes to enforcement of updated/new roles.

Our proposed framework is fundamentally different from the RBAC type approaches, as in our framework all access decisions are made based on the available information. Therefore, we can easily accommodate for the varying user roles and apply any changes to these roles in real-time.

[30] defines a dynamic role-based access control system with similar properties to our framework (such as a multiagent system with trust negotiation). However, their approach does not offer the semantic compatibility that our system provides. The trust establishment requirements are also not as flexible, requiring trust to be pre-established. Our approach is far more flexible and secure, since it requires all agents to negotiate trust on a per request basis.

### 2.2 Ontology Based Knowledge Representation & Healthcare

Ontologies have been heavily utilized in the area of medical informatics. However, the main goal of these ontologies has been to define and represent medical knowledge, and not privacy and security related concepts (as is the case in our solution).

Binfeng et al. in [3] explore building a medical knowledge base using a medical ontology for coronary heart disease. Their knowledge base has the interesting property of being able to map concepts back and forth between traditional Chinese and modern Western medical ontologies.

Cassimatis et al. in [5] argue that "Systems with human-level intelligence must both be flexible and be able to reason in an appropriate time scale. These two goals are in tension, as manifest by the contrasting properties of structured knowledge-based systems". They propose an interesting approach (reasoned unification) for representing and reasoning over linguistic and non-linguistic knowledge, within the scope of an inference context. Considering that medical information is a complex combination of various different types of data-sets, the ideas present in [5] have a significant application potential for healthcare information systems.

Another salient property of healthcare information systems is the use of many specialized domain specific ontologies by the respective specialized faculties. Therefore, in order to exchange and reason with information across all systems, we need the ability to translate the ontological concepts back and forth. [17] suggest an ontology learning framework for similar purposes. Their proposed framework provides an ontology learning environment with semi-automatic ontology-construction tools.

### 2.3 Multiagent Systems & Structured Knowledge

Semantic technologies for knowledge representation and processing seem to be very well suited for multiagent systems [6,9,11,16,28,31]. This comes as no surprise, considering that the premise of semantic knowledge representation is to facilitate machine processing of information.

[31] enhances the single coordination server limitation of the Trading Agent Competition (TAC) [25] scenario to work under the Agentcities [10] distributed agent model. Semantic web languages and tools are used to define (i)FIPA compliant ontology based agent communication language (ACL) and (ii)the knowledge-base for the agents to work with. [31]

found the use of semantic web technologies enhanced the interoperability between agents in multiagent environments.

[16] presents a very similar multiagent framework that has the ability to support multiple ontologies. Furthermore, their solution makes use of FIPA-compliant JADE agent framework to define semantic web ontology service and an inference service. These services act as middleware to support agent management, agent communication, and agent interaction protocols.

[6] proposes a ubiquitous computing system facilitating context-aware intelligent agents for the purpose of providing meaningful relevant services to individual participants in a meeting room setting. Their system is context-aware in order to personalize the user experience. The multiagent environment utilizes a semantic representation to describe the context, making it feasible for the agents to exchange and reason with the information present within the context.

[11] considers web enabled multiagent environments, where agents are distributed and provide unique services. The agents utilize customized ontologies to define and process their services. The semantic representation makes it possible for multiple agents to work together. [11] also explore the use of semantic technologies for agent communication language (ACL), where the terms used during agent-to-agent communication may originate from various ontologies.

[28] investigates the impact of agents using multiple domain specific ontologies in multiagent environments. They propose an inter-agent semantic concept learning approach to deal with the proliferation of (domain specific) ontologies. However, their solution is quite restrictive and requires closed world representation of information, where all agents are known to each other and have complete knowledge of all the information contained in the world.

Intelligent multiagent systems have been successfully utilized in healthcare settings for various applications. [9] proposes an architecture for an intelligent multiagent clinical decision support system . Although the proposed architecture is not specifically targeted for privacy and security, there are some fundamental similarities between the propose architecture in [9] and our framework (such as the use of intelligent agents to augment physician productivity in a multiagent environment).

### 2.4 Trust Management in Multiagent Systems

There are many definitions of trust when it comes to distributed systems. [21] defines trust in the context of multiagent systems as - "a belief an agent has that the other party will do what it says it will (being honest and reliable) or reciprocate (being reciprocative for the common good of both), given an opportunity to defect to get higher payoffs".

A trust relationship between two agents can be reasoned about and calculated using trust models capturing reliability and honesty of agents involved. Furthermore, an agent can define the various levels of trust it might place with another agent. [21] defines two broad categories of conceptualizing trust:

- "**Individual-level trust**, whereby an agent has some beliefs about the honesty or reciprocative nature of its interaction partners."
- "**System-level trust**, whereby the actors in the system are forced to be trustworthy by the rules of encounter (i.e. protocols and mechanisms) that regulate the system."

[12] recognizes trust as a major issue in the area of multiagent systems. Their investigation is motivated by the following three questions: (i)Why does an agent trust another? (ii)How do agents judge or evaluate the trustworthiness of others? (iii)What does an agent do after obtaining the trustworthiness of others?

[13] argues that existing trust and reputation models cannot be used for dynamic multiagent environments, where agents continuously join and leave the system. This dynamic behaviour adversely impacts the overall performance when existing trust models are used. They propose a new trust and reputation model for multiagent systems, which utilizes various forms of trust (such as role-based trust, witness reputation etc.) to produce a comprehensive score corresponding to an agent's trustworthiness.

[26] explores how non-cooperative distributed agents, when forced into working together, can utilize a trust based model to facilitate their interactions. Their mechanism focuses on two basic parameters (i)agent attributes and (ii)reliability values.

### 2.5 Electronic Consent

There are numerous studies dealing with electronic consent. However, these studies ignore the semantic aspect of information and focus mainly on security aspects [4,7,22]. O'Keefe et al. [18] undertake a feasibility study of electronic consent management systems in the medical arena. They expose various challenges faced by different consumer groups of electronic consent management systems. The study provides a sound set of recommendations for a generic implementation of a patient consent management system.

Song et al. [24] introduces the notion of an e-consent object, encompassing all relevant information concerning patient consent in the e-consent object. Lack of semantics is the biggest drawback of this model. The rules of consent are not expressed in any formal language and therefore are ambiguous at interpretation time.

Win et al. [29] describe an interface based approach through which patient consent can be expressed. The solution lacks organic growth as it hard codes the information and lacks the required flexibility for the user.

Pruski et al. [20] propose e-CRL language designed with the following two goals in mind (a)facilitate capturing of patient consent information (b)formalize the expression of patient consent information. "The language has a well defined BNF (Backus Naur Form) based syntax and semantics defined based on first-order logic and set theory which allow eHealth systems to fully control the access to critical health data" [20].

Although the e-CRL language provides support for semantics, it lacks some important features, such as proof generation. Furthermore, the defined language is not compatible with the RDF [1] based solutions and approaches, making integration difficult.

## 3 Proposed Solution

We propose a framework for exchanging sensitive patient information between multiple parties, while enforcing all required security and privacy policies along with patient consent. Our framework represents the various entities (such as hospitals, doctors, patients, staff etc.) using distributed multiagent environments, where each environment consists of intelligent agents (IAs) either representing or augmenting the functionality of an entity. All agents exist in a

cooperative mode working towards maximizing the overall system utility. We measure this system utility as the gain the patient receives from the use of our framework.

Information exchange between multiple parities is facilitated via their respective agents, where each agent takes part in a three-step information exchange handshake protocol. We currently do not address malicious agents based on the assumption that an agent's malicious activity can be detected by its corresponding environment. We utilize a semantic ontology based approach to define (a)the patient consent and (b)the privacy and security policies. The main motivation behind this approach is as follows:

- Ease of information exchange and distribution between multiple parties, while preserving the meaning of the exchanged data.
- All exchanged information is machine processable. This allows agents from different environments to not only share data with each other, but also process data in an intelligent format. Since the information is presented in a semantic format, agents can reason with the available data. They can also infer additional knowledge that might not be obvious from just the raw data.

All access decisions are processed by a semantic reasoner such as [23]. The semantic reasoner consumes the knowledge-base and the rules for knowledge inference to produce an answer for the information-access query. For each decision, the reasoner also outputs a semantic proof. This proof has a verifiability property by which any third party can compute and verify the proof independent of the proof creator. This allows us to establish trust for each access request, thus eliminating the need for pre-established trust requirements between the parties involved.

Our framework treats each access request as a single transaction. All transactions are mutually exclusive. That is to say, any previously computed access decision is not reused for the fulfilment of future requests. This allows for enforcement of all related policies on a per request basis. Therefore, a change in any policy will be applicable almost instantaneously, allowing dynamic enforcement across all environments and access requests.

Let us now discuss the details of the various components of our proposed framework.

### 3.1 Patient Consent Representation

There are many different forms of consent that a patient may choose from. Coiera and Clarke [8] define four general forms of patient consent. In our framework, we define the various types of patient consent policies (based on [8]) as follows:

- *opt-in*: A patient who has an opt-in policy allows any treating doctor to access their information.
- *opt-in-with-sensitive-documents-override*: In this case, the patient allows access to all their information except for documents that are classified as sensitive. For example, these documents may include human immunodeficiency virus (HIV) test results or sexually transmitted disease (STD) records.
- *opt-in-with-entity-override*: In this case, the patient allows access to all their information, but may specifically deny certain individuals, healthcare providers and organizations from accessing their data.

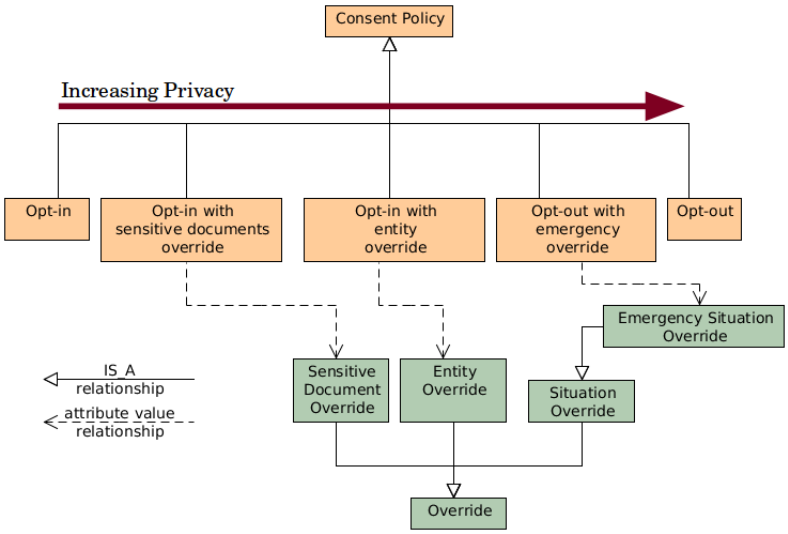


**Fig. 2.** A simple patient consent semantic model

- *opt-out*: A patient with an opt-out policy explicitly denies access to all their information regardless of who is trying to access the data or why they are trying to access it.
- *opt-out-with-emergency-override*: In this case, the patient agrees to grant access to their information only if it is an emergency situation, such as a life threatening scenario.

In order to establish a semantic representation of the above mentioned patient consent options, we need to build an ontology. It is important to note that we do not limit the type of ontology used to define patient consent. Any ontology capable of representing the core concepts (as stated above) will be acceptable by our framework. For the benefit of simplification and understanding, we define a very simple ontology model to represent patient consent concepts (please see Fig:2).

Based on our motivational example, let us assume that patient John had chosen *opt-out-with-emergency-override* as his consent policy $C_{\text{John}}$. Therefore, when Dr. Jane requests access to John's medical records from TGH, she should only be allowed access to this information if John's condition at CGH has been identified as life threatening. Otherwise, Dr. Jane's request for accessing John's medical records should be denied.

Note that for the purpose of John's consent policy, we do not really need to know the details of his life *threatening condition*. We simply need an agent at CGH to assert this fact based on the available information. Also note that this assertion will be part of the proof when executing the information exchange handshake protocol, and is also verifiable by an independent third party.

### 3.2 Privacy & Security Policy Representation

Traditionally, institutional privacy and security policies have proven to be complex in nature. This complexity is generally a function of the information and the relationships/rules defined in the policy. Therefore, an ontology based semantic representation of these policies seems like a natural choice. The overall process of translating a specific institution's policies into

its semantic representation might be time consuming, but it is not a technically challenging activity.

Similar to the consent policy, our framework supports any ontology for representing institutional privacy and security policies. The only requirement being imposed is that the selected ontology be capable of describing the relevant privacy and security concepts and their relationships.

For the purpose of clarification, we now turn back to our example under consideration. The two institutions involved are TGH and CGH. Let us assume that the privacy and security policies for these institutions are defined as follows:

- $\text{Pol}_{\text{TGH}}$ : TGH only allows employees to access patient medical records. The employee accessing patient information must also be treating the patient (or part of the team taking care of the patient). Furthermore, the employee must be on shift and must be a physician, when accessing patient information.
- $\text{Pol}_{\text{CGH}}$: CGH defines a very different and relaxed privacy and security policy. It allows access to patient medical records by all hospital employees. There are no constraints similar to the ones defined in $\text{Pol}_{\text{TGH}}$.

**Security & Privacy Axioms**: Based on John's consent ($\text{C}_{\text{John}}$) and the the institutional policies ($\text{Pol}_{\text{TGH}}$ & $\text{Pol}_{\text{CGH}}$), we can now define the following privacy and security axioms:

- All information for patient John must abide by $\{\text{C}_{\text{John}}\}$, independent of the location where the information resides.
- All information for patient John at TGH is protected by the protection set PS = $\{\text{C}_{\text{John}}$, $\text{Pol}_{\text{TGH}}\}$. Any entity or agent requesting information for patient John must provide proof of fulfilment to satisfy the set PS.
- When information is exchanged, the receiving party can augment the received protection set PS with its own privacy and security policy. Therefore, when CGH receives John's medical records, the exchanged information is now protected by a new protection set PS' = $\{\text{Pol}_{\text{CGH}}$, PS$\}$ at CGH.

### 3.3 Distributed Multiagent Environments

Our framework utilizes the multiagent systems [27] paradigm. Intelligent agents are used to either augment or replace the functionality of real world entities. For example, a physician agent can enhance the efficiency of a physician by interacting with the various information systems to collect patient data on the physician's behalf.

We group multiple intelligent agents together in an environment. All agents within a single environment are structured in hierarchical subgroups. An institution agent is the top most agent in an environment, and governs all agent interactions. We assume that all agent interactions can be monitored within the scope of an environment. By using this construct, we can define an environment for a hospital made up of supporting agents.

Agents from different environments are allowed to communicate with each other. However, all sensitive inter-environment communication should be in accordance to the information exchange handshake protocol. We have chosen to include intelligent agents in our framework for the following reasons:

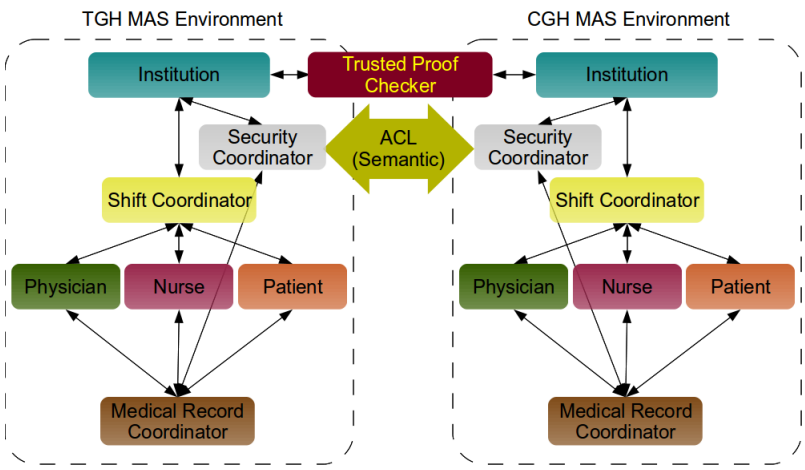


**Fig. 3.** Multiagent system healthcare environment model

- Distributed multiagent environments provide a reasonable approach to model the distributed heterogeneous healthcare institutions and healthcare providers.
- Using semantic representation of knowledge, intelligent agents can consume and process diverse data-sets from many different sources.
- A semantic reasoner can easily be integrated into an intelligent agent as opposed to an entity from the real world. This ensures complete adherence to evidence-based decision making that human agents might not be able to achieve.
- It is far easier to rely on an intelligent agent to follow all the required privacy and security protocols. All malicious activities of an intelligent agent would require breech of protocol that can easily be detected by the other agents in the environment.
- Given the same knowledge-base and reasoning rules, an agent will make the same predictable decision, hence reducing inefficiencies caused by human agent errors.
- Considering that we are proposing dynamic trust on a per request basis, it is far more efficient to utilize intelligent agents rather than human agents.

Agents utilize an agent communication language (ACL) when communicating with each other. Our framework imposes no restrictions on the choice of a particular ACL as long as the information required for successfully executing the information exchange handshake protocol can be exchanged. However, having a semantic based ACL would ensure that heterogeneous multiagent environments will be capable of communicating with each other.

We assume that all agents operate in a cooperative mode within an environment. All agents share the same utility function and work towards maximizing the overall system utility. We propose to measure this overall system utility as a function of an increase in patient privacy and security, as a result of using the multiagent system.

In support of our motivational example, we define two simple environments representing TGH and CGH (see Fig:3). The agents in both environments are similar in nature. An institutional agent governs its local environment and all encompassing agents. A security coordinator provides all privacy and security guarantees and is responsible for identifying institutional privacy and security policies. A medical record coordinator works in conjunction with the security coordinator to manage the sensitive patient information. Patients, physicians and other healthcare entities are represented by their corresponding agents. We also

define a trusted third-party proof checker agent that can be utilized to validate the semantic proofs required for information exchange, as discussed in the next section.

In order to exchange sensitive information between agents, it is desirable to have a trust relationship exist between the agents. Our framework assumes that no pre-established trust relationship exists between agents. Rather, it establishes trust on each individual request for information. The request based trust is a function of an agent's ability to satisfy the required privacy and security guarantees protecting the sensitive information that is to be exchanged. Therefore, any changes in patient consent or the institutional policies are reflected almost instantaneously.

### 3.4 Information Exchange Handshake Protocol

In our proposed framework, all information exchange between agents takes place after a successful completion of the handshake protocol. The handshake protocol is interactive in nature and requires a communication channel between all participating agents. Although synchronous real-time communication would be ideal, the protocol can be completed successfully even if the agents communicate in an asynchronous manner over any period of time. A time delay in the completion of the handshake protocol will only impact the delivery time of the requested information, and has no negative impact on the privacy and security guarantees.

The protocol has three phases that must be completed between the agent requesting the information and the agent responding to the request. We will refer to this as the request-response cycle. Given the fact that patient information may need to be aggregated from distributed heterogeneous systems, a requesting agent might engage in multiple request-response cycles with the distributed agents. Note that each request-response cycle is atomic in nature. That is to say, that an outcome of the request-response cycle does not influence the result of any other request-response cycle.

The phases of the protocol are (i)request for information (ii)proof generation and (iii)validation of the proof. These phases are described in detail as below:

***Phase 1 – Request for Information:*** This is the first phase of the protocol in which a requesting agent identifies the patient and the various sources from where the patient information is to be accessed from. Note that our framework does not constrain how this identification process is to be completed. Once identified, the requesting agent initiates one or more request-response cycles based on the number of information sources identified.

Following our example, when Dr. Jane asks for patient John's medical records from TGH, the physician agent initiates the request. Since in our framework all communication between distributed agents must be facilitated by the corresponding institutional agents, the CGH institutional agent forwards the request from Dr. Jane's physician agent to TGH. The request is processed by TGH's institutional agent by consulting with the local (security coordinator and medical record) agents to identify the protection set PS = $\{C_{John}, Pol_{TGH}\}$ (John's consent and the privacy and security policies of TGH).

The protection set PS is returned to CGH asking them to provide a proof of fulfilment for all elements in PS. This marks the completion of the first phase.

***Phase 2 – Proof Generation:*** This phase is initiated in response to receiving a protection set PS. The main goal being to mine the local knowledge-base and find evidence in

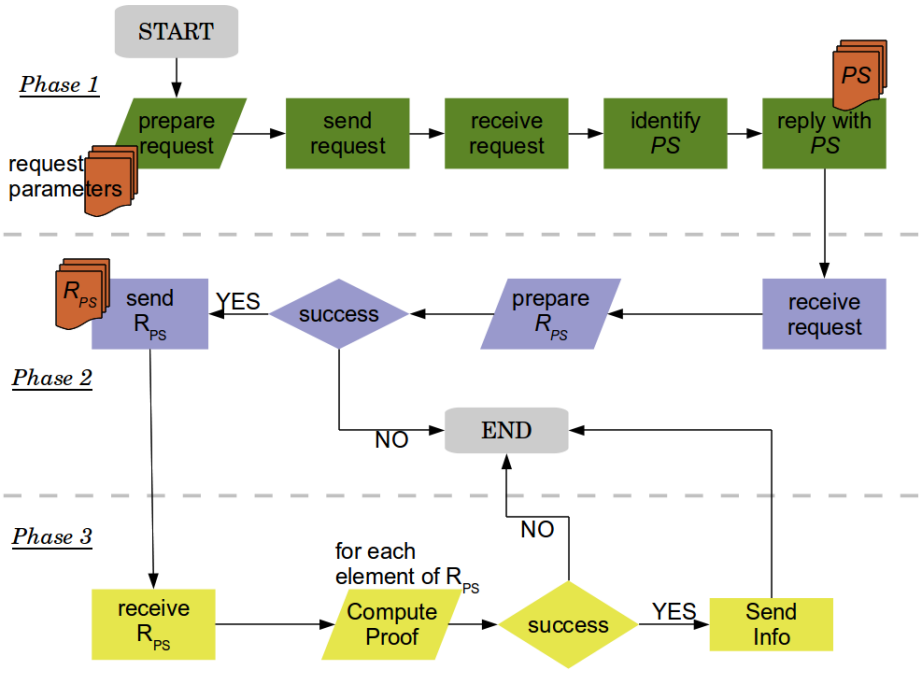


**Fig. 4.** Information exchange handshake protocol flow control.

support for fulfilment of the elements of PS. Since all our knowledge-base is represented in a machine processable semantic format, a semantic reasoner is utilized to discover facts and generate evidence from the knowledge-base. The reasoner then provides a semantic proof for the discovered knowledge.

Following our example, the CGH institutional agent will receive the protection set PS from TGH. The first element is patient John's consent that states opt-out-with-emergency-override consent policy. In conjunction with the local agents, the CGH institutional agent finds evidence that John's condition has indeed been diagnosed as life threatening. The second element in the PS represents TGH's privacy and security policy. The CGH institutional agent would then look for evidence to fulfil the requirements of $\text{Pol}_{\text{TGH}}$. It will establish that Dr. Jane (receiver of John's information) is indeed an employee of CGH, and is currently on shift and is treating patient John. Again a semantic reasoner is utilized to find the results and generate the proofs.

At this point, the CGH institutional agent has fulfilled all the requirements for PS. All the proofs are aggregated in a response set $\text{R}_{\text{PS}}$ = {P1,P2, ... Pn} which is sent back to TGH. This marks a successful completion of the second phase.

It is equally possible that the criteria in the protection set PS may not be successfully proved. For example, if Dr. Jane was not on shift, or another healthcare personnel (such as a nurse) was the initiator of the request for information. In the case of unsuccessful completion, the request-response cycle will terminate here.

***Phase 3 – Validation of Proof:*** This phase begins when the the response set $\text{R}_{\text{PS}}$ is received. Recall that the elements of $\text{R}_{\text{PS}}$ are the various proofs generated by a semantic reasoner, with the characteristic of being verifiable by any independent third party. A party

validating the proof will generally compute the proof based on the evidence found to ensure the validity of the proof.

Based on our motivational example, the TGH institutional agent will receive a response set $R_{PS}$ from CGH. It will then iterate over all the individual elements of $R_{PS}$ and validate them. In an ideal case, this validation can be performed by an independent trusted third party proof checker TTPC agent. However, the existence of a TTPC is not necessary, since the proof can be locally verified at TGH.

Upon successful completion of the request-response cycle, the requesting agent will receive the information identified in the initial request. Please refer to Fig:4 for the flow control of the information exchange handshake protocol.

## 4 Future Extensions

### 4.1 Local Ontologies

Our assumption that patient consent can be expressed using the same ontology across all multiagent environments is not practical. Each institution may use a different ontology to define its privacy and security policies. These more realistic scenarios represent a major hurdle as it nullifies the global semantic understanding of data that we require.

It is also reasonable to assume that an institution may use a hybrid ontology, where the concepts are aggregated from various other ontologies. [11] actually advocates this to be a realistic scenario given an increase in semantic technologies. Furthermore, with an increase in domain specific ontologies, agents in multiagent environments will be forced to accommodate multiple domain ontologies [28].

In order to address this weakness, we will need to augment our proposed framework with the ability to identify and map similar ontological concepts across different ontologies. There are various approaches that can be taken here. A static mapping can be pre-defined between the different ontologies, mapping the concepts from one onto the other. A better approach would be to dynamically determine if two ontological concepts are the same. This could be achieved via a detailed inspection of the attributes and relationships defined for a given concept.

### 4.2 Context-based Information

When exchanging patient information, we identify the patient, the institution holding the information and the patient medical data. We do not consider the context of the information exchange. By introducing contextual information, we can further infer as to what parts of a patient's electronic medical record might be relevant for the exchange. The notion of a context by itself is nothing new. Many other system designs are context-aware such as [6,19,31]. Therefore, this should be a simple extension to our framework with high rewards.

### 4.3 Caching and Expiration of Proof Tokens

Currently we assume that all privacy and security related information, that is compiled and/or computed to generate the required proofs, is not reused. However, if a physician agent had computed that the physician is on shift as a result of some previous proof, then

the agent could potentially cache and reuse this proof for the duration of the physician's shift.

Although caching proofs, as stated above, would greatly increase the system performance, it has potential privacy and security risks associated. For example, caching a proof that Dr. Jane is a licensed physician in Ontario, over a long period of time might not be practical since Dr. Jane could have her license revoked at any time in the future.

### 4.4 Implementation

The main concepts of our framework (such as knowledge representation, inference rules definition, automated reasoning etc.) have been individually validated using simple proof-of-concept techniques and application. For example, we utilize N3 triple (knowledge) store to define patient consent according to the simple ontology created for the purpose of demonstration. Institutional privacy and security policies are also represented as N3 statements in a triple-store. An open source semantic reasoner, Euler [23], is used to query the knowledge-base. In order to fully realize the impact of our solution, we will need to integrate it into a real world system.

## 5 Conclusion

We presented a semantic multiagent framework to enhance the privacy and security guarantees protecting sensitive medical patient data. Our proposed framework utilizes an ontological representation of patient consent and institutional privacy and security policies. These protection guarantees are communicated and satisfied before sensitive information is exchanged. We allow distributed agents to share sensitive information without having pre-established trust relationships between two parties. Our framework utilizes the trust-establishment-per-request approach to ensure real-time enforcement of any changes to either patient consent or institutional privacy and security policies. All information exchange is governed by an information exchange handshake protocol, that takes place at the beginning. The protocol ensures all protection guarantees are fully met by requiring a semantic proof for each access requirement protecting the information. This proof has a unique property that it can be validated by an independent third-party.

## References


1. Resource description framework (rdf). Website. `http://www.w3.org/RDF/`.
2. Oluwafemi Ajayi, Richard Sinnott, and Anthony Stell. Dynamic trust negotiation for flexible e-health collaborations. In *Proceedings of the 15th ACM Mardi Gras conference: From lightweight mash-ups to lambda grids: Understanding the spectrum of distributed computing requirements, applications, tools, infrastructures, interoperability, and the incremental adoption of key capabilities*, MG '08, pages 8:1–8:7, New York, NY, USA, 2008. ACM.
3. Xu Binfeng, Luo Xiaogang, Peng Chenglin, and Huang Qian. Based on ontology : Construction and application of medical knowledge base. In *Complex Medical Engineering, 2007. CME 2007. IEEE/ICME International Conference on*, pages 1586 –1589, May 2007.
4. B. Blobel. Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, 73(3):251–257, 2004.
5. N Cassimatis. Flexible inference with structured knowledge through reasoned unification. *Intelligent Systems, IEEE*, PP(99):1 –1, 2009.

6. Harry Chen, Filip Perich, Dipanjan Chakraborty, Tim Finin, and Anupam Joshi. Intelligent agents meet semantic web in a smart meeting room. *Autonomous Agents and Multiagent Systems, International Joint Conference on*, 2:854–861, 2004.
7. X. Chen, D. Berry, and W. Grimson. Identity management to support access control in e-health systems. In *4th European Conference of the International Federation for Medical and Biological Engineering*, pages 880–886. Springer, 2009.
8. E. Coiera and R. Clarke. e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association*, 11(2):129, 2004.
9. G. Czibula, I.G. Czibula, G.S. Cojocar, and A.M. Guran. Imasc - an intelligent multiagent system for clinical decision support. In *Complexity and Intelligence of the Artificial and Natural Complex Systems, Medical Applications of the Complex Systems, Biomedical Computing, 2008. CANS '08. First International Conference on*, pages 185 –190, November 2008.
10. Jonathan Dale, Steven Willmott, and Bernard Burg. Agentcities: Challenges and deployment of next-generation service environments. In *Proc. Pacific Rim Intelligent Multi-Agent Systems*, 2002.
11. James Hendler. Agents and the semantic web. *IEEE Intelligent Systems*, 16:30–37, 2001.
12. Hongbing Huang, Guiming Zhu, and Shiyao Jin. Revisiting trust and reputation in multi-agent systems. In *Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on*, volume 1, pages 424 –429, August 2008.
13. T.D. Huynh, N. R. Jennings, and N.R. Shadbolt. An integrated trust and reputation model for open multi-agent systems. *Journal of Autonomous Agents and Multi-Agent Systems*, 13(2):119–154, 2006.
14. E.H.W. Kluge. Informed consent and the security of the electronic health record (EHR): some policy considerations. *International Journal of Medical Informatics*, 73(3):229–234, 2004.
15. S. Yunkap Kwankam. What e-Health can offer. *Bulletin of the World Health Organization*, 82:800 – 802, 10 2004.
16. Jaeho Lee. Toward a practical multi-agent framework utilizing the semantic web. In *Intelligent Agents and Multi-Agent Systems*, volume 2891 of *Lecture Notes in Computer Science*, pages 122–132. Springer Berlin / Heidelberg, 2003.
17. Alexander Maedche and Steffen Staab. Ontology learning for the semantic web. *IEEE Intelligent Systems*, 16:72–79, 2001.
18. C. OKeefe, A. Goodchild, P. Greenfield, A. Waugh, E. Cheung, and D. Austin. Implementation of electronic consent mechanisms. *Final Analysis Paper*, 2002.
19. Federica Paganelli and Dino Giuli. A context-aware service platform to support continuous care networks for home-based assistance. In *Proceedings of the 4th international conference on Universal access in human-computer interaction: ambient interaction*, UAHCI'07, pages 168–177, Berlin, Heidelberg, 2007. Springer-Verlag.
20. Cedric Pruski. e-crl: A rule-based language for expressing patient electronic consent. *eHealth, Telemedicine, and Social Medicine, International Conference on*, 0:141–146, 2010.
21. Sarvapali D. Ramchurn, Dong Huynh, and Nicholas R. Jennings. Trust in multi-agent systems. *Knowl. Eng. Rev.*, 19:1–25, March 2004.
22. Jason Reid, Ian Cheong, Matthew Henricksen, and Jason Smith. A novel use of rbac to protect privacy in distributed health care information systems. In *ACISP'03: Proceedings of the 8th Australasian conference on Information security and privacy*, pages 403–415, Berlin, Heidelberg, 2003. Springer-Verlag.
23. Jos De Roo. Euler proof mechanism. Website. `http://eulersharp.sourceforge.net/`.
24. H. Song, TK Win, and P. Croll. Patient e-consent mechanism: Models and technologies. *Proceedings of CollECTeR, Melbourne, Australia*, 2002.
25. TAC Team, Michael P. Wellman, Peter R. Wurman, Kevin O'Malley, Roshan Bangera, Shou-de Lin, Daniel Reeves, and William E. Walsh. Designing the market game for a trading agent competition. *IEEE Internet Computing*, 5:43–51, March 2001.
26. A. Terauchi and O. Akashi. Trust-based cooperative action control in multi-agent systems for network management. In *Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on*, pages 278 –283, May 2009.
27. Gerhard Weiss, editor. *Multiagent systems: a modern approach to distributed artificial intelligence*. MIT Press, Cambridge, MA, USA, 1999.
28. Andrew B. Williams. Learning to share meaning in a multi-agent system. *Autonomous Agents and Multi-Agent Systems*, 8:165–193, March 2004.
29. K. Win, H. Song, P. Croll, and J. Cooper. Implementing patient's consent in electronic health record systems. *Proceedings of CollECTeR, Melbourne, Australia*, 2002.
30. Jae Wook Woo, Myung Jin Hwang, Chun Gyeong Lee, and Hee Yong Youn. Dynamic role-based access control with trust-satisfaction and reputation for multi-agent system. In *Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on*, pages 1121 –1126, 4 2010.

31. Youyong Zou, Tim Finin, Li Ding, Harry Chen, and Rong Pan. Using Semantic web technology in Multi-Agent systems: a case study in the TAGA Trading agent environment. In *Proceeding of the 5th International Conference on Electronic Commerce*, pages 95–101, September 2003.