Intelligent Information Management, 2012, 4, 401-406
http://dx.doi.org/10.4236/iim.2012.46045 Published Online November 2012 (http://www.SciRP.org/journal/iim)

Trust and Security on Semantic HIM (Health Information Management)

Nasim Khozouei[1], Razie Vanda[2], Peyman Khozouei[1]
[1]Department of Computer Engineering, Yasuj Branch, Islamic Azad University, Yasuj, Iran
[2]Department of Gynecology and Obstetrics, Medical University of Yasuj, Yasuj, Iran
Email: n_khozooyi2003@yahoo.com, pmnkh@yahoo.com

Received August 8, 2012; revised September 8, 2012; accepted September 15, 2012

ABSTRACT

Information technology have changed information media by networking and internet using technology in health as same as another part improve efficiency and effectiveness. Currently, the medical document is reality-based medicine, so that is the most important, richest and the most realistic source of medical and health information. Health information management systems that require systems to the storage, retrieval, storage and elimination of health records (by law), and adjust to the rules of professional. These processes are difficult and time consuming for human. In the meantime semantic HIM seem best solution.

Keywords: Health Information Management (HIM); Medical Document; Health Information System(HIS); Semantic Web; Security; Trust

1. Introduction

Resource management activities are information. Information flow is vital to the planning process. Today, one of the most important powers in the world is information. Managers without having complete information about a subject will not be able to influence decisions. Information technology have changed information media by networking and internet using technology in health as same as another part improve efficiency and effectiveness. In technology century the medical document is Reality-based medicine, so that is the most important, richest and the most realistic source of medical and health information.

The health information management include development, implementation, maintenance, and management systems for production, storage, retrieval and dissemination of patient health information, effectively and efficiently.

In fact, information based decision making and planning is the primary source of information about health care, the patient is a health certificate.

Medical records manual or automated form, have medical information in all aspects of patient care, physicians, nurses and other health care providers need to treat a patient's medical Information. Medical document, also to protect the interests of patients, health care, health care centers that serve. Health information management systems that require systems to the storage, retrieval, storage and elimination of health records (by law), and adjust to the rules of professional. Today, traditional methods of storage retention and retrieval of medical information is not sufficient.

Currently, Health Information Management Association (AHIMA) American Health Information Management is to provide a new definition:

Management Information Systems HIS, a sub-system of health information systems that are dedicated to system management. And system logs, critical care, epidemiology and other are examples of these sub-systems.

2. Medical Documents or "Health Information System"

Medical documents or "health information system" include: All information regarding is a person's health, which includes sociology, pathology.

The medical records of patients and mostly is stored in the form by computer. And are available in need of treatment, research, medical education and health, evaluating health services, legal issues and… like Information such as type of disease, treatment, therapies performed, type of surgery, the patient's discharge status-health information and…

2.1. The Health Information Technicians

Health information technician, performs a variety of technical tasks on health information like:

- Coding and classification of information for reimbursement;
- Organize, analyze and evaluate information needed for decision support;
- Security information for use in community health care;
- Standards and regulations related to health information;
- Provide health information to validate analysis;
- Analysis of clinical data for research and public policy.

2.2. Document Management, Medical Records Documenting

- Continuous monitoring of the documents;
- Ensure that only the documents needed to be created;
- The documents are well protected;
- Properly and effectively used;
- What is worthless, will fade;
- Valuable documents in the National Archives Act shall keep and maintain according to (Bateni, 1374, page 89).

Management medical documentation will be difficult for human, and the analysis and conclusions from the data would be very time consuming. So there seems to be essential to an intelligent network technology.

3. Semantic Web

The Semantic Web aims at machine-processable information. The step from the current Web to the Semantic Web is the step from the manual to the automatic processing of information. This step is comparable to the step from the manual processing of information to the machine processing of information at the beginning of the documentation revolution. Hence, the Semantic Web can be seen as the dawn of the informational revolution [1].

The Semantic Web enables automated intelligent services. The Semantic Web, which contains machine-processable information, will enable further levels of software-system interoperability.

Technology and standards need to be defined not only for the syntactic representation of documents (like HTML), but also for their semantic content. Semantic interoperability is facilitated by recent W3C standardization efforts, notably XML/XML Schema, RDF/RDF Schema and OWL. The technology stack envisioned by the W3C is depicted in **Figure 1**. Apparently, XML as well as XML Schema are the second layer above URIs and Unicode. The third layer is RDF and RDFS. The next layer is the ontology language [2].

3.1. Secure E-HIM

Because of the different components, operations, resources and users, computer networks and especially web becoming a very convenient target for attacks and illegal operations in electronic health Information managements. So e-HIM application developers should develop formalized security model during application developments as part of a security architecture methodology and risk analysis for all e-HIM systems to ensure that they are protected according to their stated security requirements and identified risk [3].

Secure Health Information management is also a key aspect of secure management. Health Information management is useful in several areas in integration for many domains including medical, insurance, and intelligence. Some of the information exchanged between organizations may be highly sensitive, especially for military and intelligence applications. There needs to be a way to protect such sensitive information. Because the transacttions are carried out on the Web, a combination of access-control rules and encryption techniques are being proposed as solutions for protecting sensitive information for Health Information management.

We define the Information Protection and Security as: "The application of policies, procedures, and technology to protect Information assets (integration, categories, facilities, equipment, information, and insurance organization) from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people, etc."

Technologies may change, but the essential requirements remain much the same, comprising the key concepts of Authentication, Authorization, Integrity, Signature, Confidentiality, Privacy, and more recently, Digital Rights Management and Information Rights management to secure e-HIS **Table 1** summarizes the meaning of these concepts.

If we make progress for secure Web information-management technologies, we can vastly improve the security of e-HIS transactions. The next section will elaborate on semantic Web technologies for e-HIS. The integration of e-HIS with the semantic Web has come to be known as semantic e-HIS.

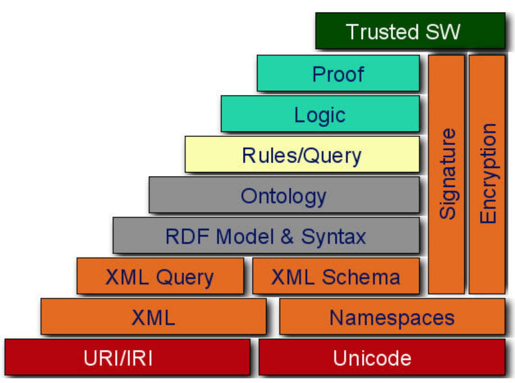

Figure 1. Basis of the semantic Web.

Table 1. Summary of essential security concepts for e-HIM.

Concept	Question answered	Comment
Authentication	Who am I?(Verify asserted identity against some trusted authority)	Thelater trust section further discuses authentication, identify, and role issues.
Authority Integrity	What may I access and do? Is the information intact?	Individual and role. See above Prevent accidental or malicious change, or at least detect it.
Signature	Is the information certificated?	Ties in with identify issue. Might certify an identity or athority.
Confidentiality	Is the information safe from unauthorized disclosure?	Encryption makes information unreadable even if access controls and circumvented.
Privacy	Is individual and sensitive information safe from unauthorized disclosure?	Governance issue of how to use sensitive information. Consent.
Digital Right Managment	How may I use or share this information?	Usually now combination of access control and embedded enforcement of usage license.

3.2. Secure Semantic HIM

The semantic Web has been applied to e-HIM in two major directions. One is developing specialized markup languages such as Electronic Business using eXtensible Markup Language (ebXML) for e-HIM applications, and the other is semantic e-HIM where e-HIM processes make use of semantic Web technologies.

In this section we will discuss both directions and then examine the security impact. As stated in Reference [4], ebXML "is a family of XML-based standards sponsored by OASIS and UN/CEFACT, whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic medical information in an interoperable, secure, and consistent manner by all hospital and insurance partners".

The initial goal of this project was to specify XML standards for medical processes. These standards include:

- Standard for integration information like abbreviation, prognosis and cure according to ICD;
- Standard for analysis information to decided;
- Standard for hospital and insurance collaboration.

Ontologies can also be developed for e-HIM applications specified in languages such as Resource Description Framework (RDF), RDF-S, and Web Ontology Language (OWL), and OWL-S.

It essentially integrates semantic Web technologies with medical process management and knowledge management in HIM. The medical processes utilize knowledge management to improve their efficiency and utility and use semantic Web technologies such as ontologies for better understanding.

Semantic medical, which is more or less semantic e-HIM, is also being investigated. The semantic Web can support a service description language that can be used throughout this life cycle. By using Markup Language + Ontology Interface Language, we have been able to develop a service description language that is useful not only to represent advertisements, but also implement matchmaking queries, negotiation proposals, and agreements [5].

There is some work on security for various standards such as Web services. However, trustworthy semantic Web technologies, which include not only confidentiality, but also privacy, trust, and integrity among others, need more examination for the various standards that are evolving [Thur-2008]. For many of the e-HIM applications for surgery there are complex contracts and negotiations between different physicians, and therefore we need more research on expressing policies and reasoning about the policies. However, what we need is to incorporate the research into the standards and specifications so that information based on these standards can be used in an operational environment **Figure 2** illustrates aspects of secure semantic HIM.

Recognizing that information security and privacy play an increasingly important role in a HIM in which the Web is central to exchange information, between hospitals and another medical organization, and education, several OWL-S categories have been proposed and developed to resolve such issues:

- Credential Ontology defines the capability to specify access control restrictions of Web pages or Web services that use authentication as a requirement for authorized access in HIM;
- Security Mechanisms Ontology defines the capability to interface on a high level of abstraction among various security standards and notations;

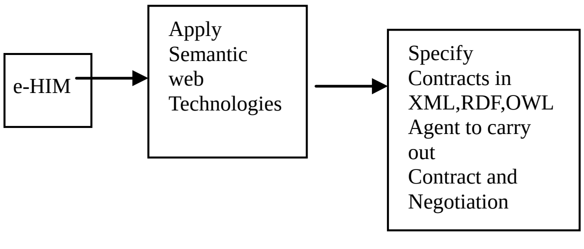

Figure 2. Aspects of secure semantic HIM.

- Service Security Extensions Ontology defines the capability to annotate the security properties of SWS;
- Agent Security Extensions Ontology defines the capability to annotate the security properties of agents;
- Privacy Ontology defines the capability to express privacy policies to protect information, and a protocol to support matching of privacy policies across different contexts;
- Cryptographically Annotated Information Object Ontology defines the capability to capture encrypted or signed input or output data of services.

One may see these efforts as a measure of technology maturity on the road to implementing practical services to realize the greater swab vision.

Another essential requirement of security standards in the Web context is that they work naturally with content created using XML (or with XML-derived languages and protocols) [6].

Transparency is another essential characteristic, in that integrity, confidentiality, and other security benefits should apply to XML resources without preventing further processing by standard XML tools—whether at message endpoints, or in intermediate processing.

Although older security technologies provide a core set of security algorithms and technologies that can be used in XML contexts, the actual implementation of these is inappropriate for most XML applications:

- The proprietary binary formats require specialized software for interpretation and use, even just to extract portions of the security information;
- Older technologies tend to assume specific components integrated into the endpoint applications, introducing awkward dependencies;
- Older standards are not designed for use with XML and thus lack support for common;
- XML techniques for managing content (such as URI or XPath pointers).

A unified and open framework of new web-oriented standards and implementations, however, is evolving to address these issues on the Web.

Since public and corporate awareness seems dominated by a focus on Microsoft's. NET solutions, it is important to explore the subject in general terms. In particular, we need to highlight the alternatives to central authentication by proxy authorities, with their proprietary interpretations of "trust" and "security" as a "product" to sell, in order to assess properly the role of these concepts in the broader Semantic Web context.

4. Trust on Semantic Web

4.1. Why Do We Need "Trust"?

The Semantic Web whilst difficult for most people to conceive, is simply an extension of the Web as many people currently know it. As a distributed document retrieval system, the Web allows any party to publish information, and to make this information available to any other party (or restrict access as they see fit). The Semantic Web uses this system of protocols as its core means of communication, but places a web of linked, machine understandable data on top of the document retrieval abilities of the Web [7].

4.2. An Introduction to Trust

Trust of the Semantic Web is that automated "hospital" will be able to search through the distributed databases available, and be able to process this data in intelligent ways [7], using more advanced techniques than those currently used in data processing (for example, Patient-records).

The Semantic Web is a vision which seeks to enable a generation of computers and applications which work better for their users, by providing the information that those computers need in a rich format.

On the Web, it is up to the user (who reads web pages directly) to determine whether or not the information published by a web page is either credible or trustworthy. This decision is often made with relative ease by skilled and experienced users and previous studies which examine how users determine the credibility of a web page which they are reading at. For an automated hospital, blindly trusting information which is obtained from the Web may lead to inaccurate or incorrect conclusions. The patient may not question the results that the physician presents (perhaps due to a blind trust in technology [7], or it may be difficult to diagnose which data or step of reasoning caused the physician to present incorrect results to the patient. It is therefore important that an automated hospital is able to assess the credibility of each component of data it has obtained from the Web in order to determine whether it should use the information for further processing or not.

The decision of whether or not a piece of data is credible is a difficult decision for an automated hospital to make, as it is unable to properly take into account either the context of the information, or some of the heuristics which a human user of the Web may employ to examine the source and quality of the information presented to them.

Automated hospital such as these will be prevalent on the Semantic Web, and without a means of automatically assessing the credibility of information which they have gathered, the utility of such automated agents may be drastically reduced.

4.3. What Is Trust?

While some work has been done on the topic of trust in information systems, the author believes that his initial thoughts about the topic are worth examining, as they indicate the essence of the work which he is trying to do, without clouding the issue with formal definitions, or definitions which are appropriate for other works. The discussion will return to other, more fully investigated definitions later in order to arrive at a final conclusion.

As mentioned above, an hospital on the Semantic Web needs to be able to decide whether data it.

4.4. An Introduction to Trust

Obtains from the Web is fit for further processing, where its "fitness" is not yet a clearly defined concept. Importantly, this fitness is the fitness of the data which is obtained, rather than trust of the person or system which generated the data. However, an assessment of every piece of data is unrealistic, and assessing an author (human or machine) is a practical means of classifying the information which that author has published.

Briefly (and with the understanding that this definition is a preconception), the author's notion is that trust is the belief that data is accurate, or fulfills criteria which the consumer believes it should [8].

4.5. Trust on the Semantic Web

With a clear understanding of what the Semantic Web is, and the technologies on which it is based, and as you now what trust is, and ways in which it may be modelled, a discussion on trust and the Semantic Web together is possible.

The Web is a distributed information space, where anybody may publish any information they desire. The Semantic Web does not change the underlying protocols (like HTTP [7]) or the very basis of the Web, the URI [7], and is thus still an information space (tied together with URIs) where anybody may publish information (retrieved by HTTP).

As we know, people assess the credibility of information retrieved from the Web in a number of ways, including visual clues such as the design of the site.

On the Semantic Web, information is data with a simple form, and is designed to be processed by computers, which means that many of the means used to assess credibility on the Web are not applicable on the Semantic Web.

On the Semantic Web, data should be assessed for trustworthiness before it is processed, so that results presented to the user (based, perhaps on many data sources) is accurate. Without a reasonable belief that a system will present accurate results, uptake of Semantic Web based technologies is not likely to be high. Golbeck *et al.* have produced the most trust research relating to the Semantic Web. Golbeck's greatest contributions in the area are two trust metrics which have been tested and measured [7], and an RDF vocabulary for describing trust relationships on the Semantic Web [7]. Trust must be distributed. That is, each hospital in the system has a unique perspective on the trustworthiness of other agents. Golbeck's trust metric is distributed in this sense, and in the sense that publication of trust values can be distributed and published like any other document published on the Web.

4.6. The Trust Ontology

The trust ontology is designed to extend the FOAF ontology, allowing users to describe how much they trust other people, in general or in a particular domain.

The ontology has changed compared to the description given in [7] and the description (and URI) given in [7]. The ontology as it is currently published and described online [7] is the ontology has a trust rating scale of 1 to 10, with no notion of explicit distrust, and allows the optional description of trust in specific knowledge domains. **Figure 3** provides an example of both uses.

Figure 3 contains two trust statements. The first uses the trusts regarding form to state that a foaf: Person with the name "Jen Golbeck" is trusted regarding the trust subject which has a URI of http://trust.mindswap.org, with a trust Value of 10. The second, simpler, form of a trust statement simply states that the first person has a trust10 property, with a value of a foaf: Person with the name of "Barry Irwin". This statement means that the first person trusts the second with a value of 10 in all knowledge domains.

By allowing the explicit statement of trust using Semantic Web technologies, the trust ontology goes some way towards allowing the description of trust on the Semantic Web. With an openly usable description of trust values available, it is conceivable that the data could be aggregated and reused by a service which would infer trust ratings for as yet unknown users.

4.7. A Trusted Semantic HIM

Credibility of Web sites has become a concern amongst those who believe that the Web is a powerful tool, and

```
@prefix trust: <http://trust.mindswap.org/ont/trust.owl
:a rdf:type foaf:Person .
:a trust:trustsRegarding :b .
:b trust:trust Subject <http://trust.mindswap.org/> .
:b trust:trustedPerson :c .
:c rdf:type foaf:Person .
:c foaf:name "Jen Golbeck" .
:b trust:trust Value 10 .
:a trust:trust10 :d .
:d rdf:type foaf:Person .
:d foaf :name "Barry Irwin"
```

Figure 3. An RDF snippet in N3 showing example usage of the trust ontology.

has even lead to the formation of organisations such as Consumer Reports Web Watch [7], which "seeks to improve the credibility of content on the World Wide Web".

A part of the problem is that users may find they are unable to trust, in general, content found online if the Semantic Web is to overcome this problem, the system, as a whole, must be seen as trustworthy, and must be largely resistant to common current attacks and problems, such as phishing and spam.

The Semantic Web stack, illustrates the technologies required to build a trusted Semantic Web. Key to this diagram is the placement of signature and encryption, which lie alongside the serialisation, logical model, ontology, query, logic and proof layers. Only together with the ability to prove where results originated, with reporting on the logic used to arrive at a result, will a truly trusted Semantic Web exist. The implication of this is that digital signature and encryption will be required to work with other technologies in order to support a Semantic Web in which users will be able to place their trust [9].

There are possible solutions for this problem, although it is beyond the scope of this work, and potential solutions are therefore not properly investigated. An authentication mechanism which only allows friends to get information about other friends (and not themselves) may be possible.

This, however, would limit the depth of a distributed social network to two links away from the source, a major problem. As above, it would also disallow people with no authorisation from accessing the information, otherwise friends could simply access the information without login credentials to reveal the "secret" information, potentially leading to a breakdown in trust networks.

5. Conclusions

This paper has provided an overview of security and trust on e-HIM and then discussed various aspects of secure semantic HIM. Semantic HIM essentially integrates semantic Web technologies with process management and knowledge management in information management. We also discussed some of the key points in ebXML, the XML standard for trust on semantic HIM applications. Finally, we examined the security and trust impact on semantic HIM.

The discussion in this paper is preliminary because much of the research in semantic HIM in general and security and trust semantic HIM in particular is in the early stages. We believe that it is important to investigate security while the semantic HIM standards are being developed. As we have discussed, several trust ontologies for HIM applications are being developed. These ontologies have to be extended to specify various confidentiality, privacy, and trust policies. Information management on semantic web applications will likely have complex policies as transactions are carried out between multiple medical organizations and insurance organization.

Therefore, we need languages to specify the policies and reasoning engines to reason about the policies. We need to examine languages for confidentiality, privacy, and trust policy management of HIM applications.

REFERENCES

[1] C. C. Poirier, *et al.*, "E-supply Chain: Using the Internet to Revolutionize Your Business," San Francisco, 2000.

[2] T. Berners-Lee, J. Hendler and O. Lassila, "The Semantic Web," *Scientific American*, 2001, pp. 29-37.

[3] M. A. Mahmood, *et al.*, "Reengineering Supply Chain Management: An E-Commerce Approach, Issues and Trends of IT Management in Contemporary Organizations," 2002.

[4] eBXML, 2009. http://en.wikipedia.org/wiki/EbXML

[5] D. Trastour, *et al.*, "Semantic Web Support for the Business-to-Business E-Commerce Lifecycle," 2002. http://www2002.org/CDROM/refereed/211

[6] B. Thuraisingham, "Building Trustworthy Semantic Webs," *IEEE International Conference on Information Reuse & Integration*, 2009, Las Vegas, 10-12 August 2009, pp. 10-12.

[7] M. Richardson, R. Agrawal and P. Domingos, "Trust Management for the Semantic Web," *The Semantic Web—ISWC* 2003, Sanibel Island, Vol. 2870, 2003, pp. 351-368. http://link.springer.com/book/10.1007/b14287

[8] B. Thuraisingham, "Directions for Security and Privacy for Semantic E-Business Applications," *Communications of the ACM—The Semantic E-Business Vision*, Vol. 48, No. 12, 2005, pp. 71-73. doi:10.1145/1101779.1101812

[9] R. Ganeshan, *et al.*, "An Introduction to Supply Chain Management," 1995.