

HEALTH INFORMATION MANAGEMENT ON SEMANTIC WEB :(SEMANTIC HIM)

Nasim Khozoie

Department of Computer Engineering, yasuj branch,
Islamic Azad University, yasuj, Iran
n_khozooyi2003@yahoo.com

ABSTRACT

Information technology have changed information media by networking and internet .using technology in health as same as another part improve effcieincy and effectivness. 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 process are difficult and time consumig 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 is information. Information flow is vital to the planning process. Today, one of the most important power 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 effcieincy and effectivness . 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 this 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. 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 Fig. 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 [5].

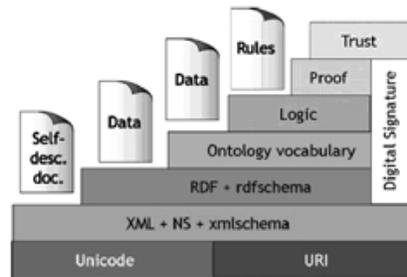


Fig. 1 Basis of the semantic Web

On top of the ontology language, there is a need for a language to express logic, so that information can be inferred and better put into relation. Once there is logic, it makes sense to use it to prove things. The proof layer enables everyone to write logic statements, and an agent can follow these semantic “links” to construct proofs, so that validity of a statement, especially an inferred statement, can be checked. The proof layer combined with digital signatures will lead to trust. Consequently, ontology and ontology-based meta data are the basic ingredients for the Semantic Web layer cake. An important question is therefore how to create and use ontology and ontology-based meta data.

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.

Secure Health Information management is also a key aspect of secure Managment. Health Information management is useful in several areas in integration for many domains including medical, insurancr, 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 transactions 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 organizaion) 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.

TABLE1
Summary of essential security concepts for e-HIM

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

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.

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 [6], 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 [7].

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 surjery there are complex contracts and negotiations between different phisicians, 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.

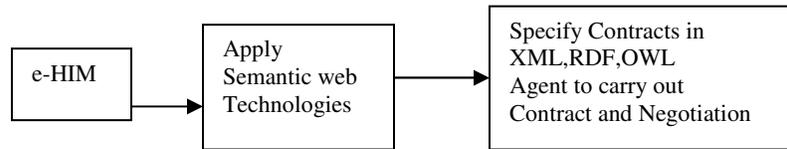


Fig. 2 Aspects of secure semantic HIM.

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.
- 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)[8].

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 sweb-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. CONCLUSIONS

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

The discussion in this paper is preliminary because much of the research in semantic HIM in general and secure 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 ontologies for HIM applications are being developed. These ontologies have to be extended to specify various confidentiality, privacy, and trust policies. Business 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] Thuraisingham, B, 2005, *Security and privacy for semantic E-business*, Commn, Assoc. Computer Machinery, 48(12): 71–73.
- [2] R Ganeshan. Et al.1995, *An introduction to supply chain management*, mason.wm.edu.
- [3] Poirier, C. C, et al. 2000, *E-supply Chain: Using the Internet to Revolutionize Your Business*, San Francisco.
- [4] Mahmood M. A.,et al 2002, *Reengineering Supply Chain Management: An E-Commerce Approach*, Issues and Trends of IT Management in Contemporary Organizations.

- [5] Berners-Lee, et al. 2001, *The Semantic Web*, Scientific American Magazine. <http://www.sciam.com/article.cfm?id=the-semantic-web&print=true>. Accessed 20 November 2009.
- [6] *eBXML*, <http://en.wikipedia.org/wiki/EbXML>, Accessed 10 September 2009.
- [7] Trastour D et al, 2002, *Semantic Web Support for the Business-to-Business E-Commerce Lifecycle*, <http://www2002.org/CDROM/refereed/211/>.
- [8] Thuraisingham, "Building Trustworthy Semantic Webs"; Auerbach; 2008

Authors : Nasim KHOZOIE

Biography:

I, originally from Iran, I have been studying about semantic web since 2009. I have graduated from Shiraz State University in IT (Master degree) at 2009. I had written several papers in semantic web topics, such as: Management of semantic web- Dubai-Dec2009(ICCEE) print&presentation security in SCM -Amsterdam -September 2010 print&presentation e learning on semantic web 7 -9, January 2011, Mumbai, India(ICEo4) print&presentation and in another topic, like: Security in Mobile Governmental Transactions -Dubai-Dec2009(ICCEE Dec2009(ICCEE) print&presentation E-cash ,Iran, 1388(2009)



....

furthermore I do multi tasking smart card project (national project) and
also I'm member of scientific board of Islamic Azad University, I'm teaching database course , Internet& network course ,....