Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 192 – 198

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Issues in Achieving Complete Interoperability while Sharing Electronic Health Records

Shalini Bhartiya[a]*, Deepti Mehrotra[a], Anup Girdhar[b]

[a]*Amity University, Uttar Pradesh, Sector-125, NOIDA, U.P. INDIA*
[b]*Sedulity Goups, Suneja Towers, Janakpuri, New Delhi, INDIA*

Abstract

Accessing health data and sharing with the team of professionals for providing continuity of care is a primary activity in healthcare environment. Enormous and frequent access, questions the measures adopted in maintaining confidentiality and privacy of patients Electronic Health Records (EHRs). Heterogeneity in EHRs and EHR systems introduce further complexities and restrictions to share data between independent hospitals or health-professionals. The problems of semantics, the difference between bounded and unbounded software systems and ascertaining security while sharing data add to the difficulty of achieving interoperability. This paper identifies various approaches and issues in achieving interoperability while sharing of EHRs.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Interoperability; Syntactic Interoperability; Semantic Interoperability; Electronic Health Records; Security

1. Introduction

"Interoperability[1, 2] is the ability of two or more components, applications or systems to exchange and use information". E-health records has merged as a backbone of Hospital Information system (HIS) and complete usage of EHR can be achieved in an interoperable environment. Also, in near future, an exponential growth in sharing of EHR is expected. Interoperability of Electronic Health Record (EHR) defined in ISO[3] as "the ability of two or more applications being able to communicate in an effective manner without compromising the content of transmitted

* Corresponding author. Tel.: +919717388700
E-mail address:shalinibhartiya69@gmail.com

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.033

EHR." The optimal usage of EHR can be achieved by making it accessible to the patient/doctor or any other end-user well in time. The EHR can be shared within the units of the hospital (intra-sharing) or between different hospitals (inter-sharing) particularly, laboratories and other external agencies such as insurance and government research units. Thus, there need to design an environment which supports interoperability. In context of interoperability, key security issues are: whom to share, how much to share, how to share such that no unauthorized access can be made to any data.

EHRs need to be fragmented according to the requirements of the user. Along with determining a purpose-based fragmentation of EHR, identifying the end-user of the fragmented EHR is equally important. In healthcare domain, one user works in different role-capacity at any given point of time. For ex., a doctor may be a primary doctor for one patient and act as specialist for another patient. This difference complements specific access of patient's data as per the role and responsibility. Another important factor is the assignment of authorized signatory permitting legitimate access to the required data. As the hierarchy and authority is not static as for ex., a doctor can work as a member of team controlled by a consultant or can work independently in the same hospital, the accountability and responsibility is difficult to ascertain. Hence, it is challenging to determine authorized and consolidated access to EHRs. Also, interoperable problems of naming conflicts and resolving dependencies between different attributes of disparate access control policies requires evaluation of such attributes to implement two separated layers of syntactic and semantic validation. Thus, a dynamic feedback to the system must be provided that further runs a specific algorithm necessary to solve any possible conflicts.

Today, most healthcare applications use or create HL7 or ANSI X12 messages for sharing of data. This "common language" allows healthcare organizations to integrate different applications with the support of existing IT environment in the organization. Another challenge is ensuring confidentiality and privacy of patient's sensitive health records shared within departments both in closed as well as open networks.

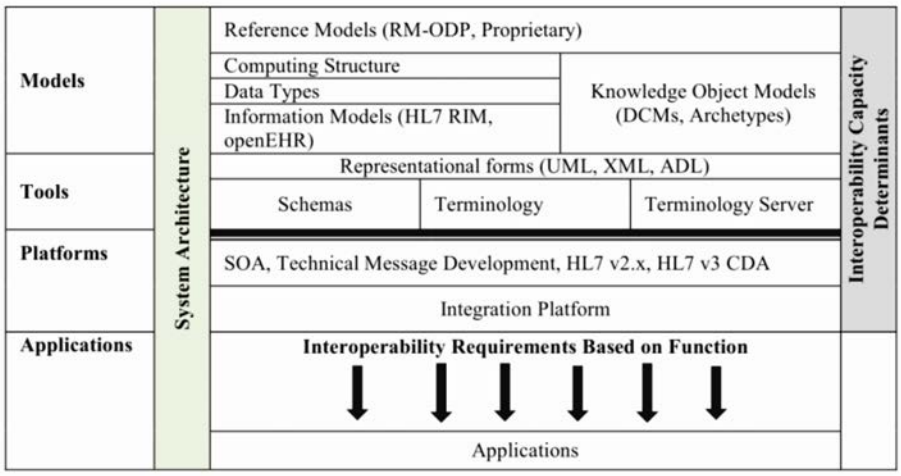

Fig.1. Architecture of Interoperable EHR-Systems[4]

Fig.1 illustrates the architecture of interoperable data sharing. The thick line alienates semantic and syntactic interoperability. The semantic interoperability lies above the line that represents the models and tools much specifically used in designing data interoperable platform. Syntactic interoperability incorporates designing of the platform or interfaces compatible with the specified guidelines in the concerned domain. The applications collaborate with the help of interoperable functions and allow data sharing. Semantic interoperability is a mechanism to interpret information whereas syntactic and structural interoperability describes data in a uniform way for allowing automatic processing of shared information with ease. The relationship between two is inclusive[4]: *a pattern semantically valid will always be syntactically valid, but not the other way around*. Smooth and secured data transition between heterogeneous EHR-systems requires correct and accurate syntactic interoperability. Syntactic matching of attributes consists of syntactically comparing attribute values. However, the syntactic matching has significant limitation such as false positive and false negative answers. Semantic issues need to be assessed from

different angles and viewpoints. Resolving semantic differences requires that trenchant differences be resolved in a universal manner. Different frameworks distinctly emphasize the effect of semantic interoperability that must be individually examined for achieving compatibility and integrity of sharable information.

With respect to securing EHRs, the Health Insurance Privacy and Accountability Act[5] Security Rule necessitates setting up of various safeguards - physical, administrative, and technical, to protect electronic health information. National Institute of Standards and Technology[6] has developed guidelines applying appropriate levels of security according to impact or consequences that might result from the unauthorized disclosure or modification of EHR-system. The guidelines are based on review of categorization of security terms and definitions by FIPS 199. World Health Organization[7] has given guidelines about how to review the current health record systems before discussing issues and challenges to the security of EHR. Effort is required to incorporate compliance like HIPAA security guidance with own security policies in standardization of EHR systems at the national and international level.

The commonly selected approaches[8, 9] that drive interoperability entail various merits and demerits with respect to interoperability and compatibility in respective areas of their applicability. Some generic models of interoperability have been proposed by researchers[10, 11] focusing on semantic, syntactic and structural interoperability. Securing data requires enabling and managing of syntactic and semantic interoperability[12] which is challenging due to the need of high alignment among disparate systems.

2. Securing data and Managing Syntactic and Semantic Interoperability

2.1. Layered Approach

The gap between the syntactic and semantic interoperability can be reduced by harnessing a layered approach[13] that resembles the principles of networking. The layers can be categorized as- Syntax layer, object layer and the Semantic layer. Each layer has a number of sub-layers that correspond to a specific data modeling feature. The data is correctly interpreted at each layer to be later passed to the next layer. Each layer relies on a number of rules and conventions to share data with the peer systems on the network. The challenge to this approach is clearly distinguishing between the layers or features prevalent in the sub-layers. Moreover, it is difficult to establish relationship and dependencies between each layer that may exist in given systems. It is equally difficult to build flexible interfaces enabling user friendly communication between disparate systems.

2.2. Centralized Approach

Keeping the data at a single place or location appears to be easy to manage and control. It heads towards creation of generic model[14] independent of any specific architecture or schema. The basic strategy used in designing such approach is to generate templates that can be dynamically changed as per the suitability of the particular application and environment. The syntactic and semantic interoperability is achieved through servers designed on highly flexible client-server architecture. Though it encompass the advantages of wide access of data, it is extensively difficult to manage and maintain the shared data across multiple platforms and applications. Moreover, centralized approach is more vulnerable with respect to data breach as it entails multiple points of access at which the user information can be submitted and received.

2.3. Decentralized Approach

In coordination with the heterogeneous nature of data and applications, another suitable approach considered is the decentralized approach. In this approach[14], each system maintains its own repository of data model and architecture independently. Various fragments of such models integrate and share the data as per their adaptability of the current environment and schemas. This approach is highly dynamic and generates unpredictable results on collaborating disparate systems. The systems communicate directly in a peer-to-peer manner at the time of sharing the data. The data can be shared without assuming shared meanings but rather enabling dynamic translations of inputted terms. This mechanism enables more functionalities and security as each system incorporates defines its

own privacy policies for sharing the data. The decentralized approach gives rise to the number of policy conflicts that arise due to the existence of conflicting rules in disparate access control policies of each system.

2.4. Similarity-based Approach

Establishing similarities requires comparing contextual attributes or components of two or more objects, described in the given language that links the semantic and schematic level. Similarity is the confidence measure between two elements in different user hierarchies. The similarity is expressed in a mathematical number that typically range in [0-1]. A framework[15] is proposed for ranking the users and the resources on the basis of their hierarchical positions in their organizations. The relevant and authorized access is matched on merging of disparate access privileges of the users and permissions granted accordingly. It evaluates the degree of similarity between two or more user's ranks from defined attributes in the access control policies of each user. The similarity score obtained on measuring the hierarchical distance between each user generates a unique value utilized as security level (SL) for each user/resource attribute in the defined access control policies of heterogeneous healthcare systems. A similarity score 0 implies that no matching holds between the attributes. The framework extends the usage of similarity score by defining the authorization on the basis of the hierarchical positions and the roles defined in the given policies.

3. Case Study

Data sharing between two or more disparate systems is visualized in healthcare domain. Two hospitals A and B, having their data stored in their databases, dbA and dbB respectively and also having independent set of access control policies, collaborate to share patient's health records under the authorization and consent of the patient. Figure 2 depicts the architectural view of this collaboration in approaches described in section 2. Fig. 2(a) shows A and B sharing authorized data using layered approach. EHR-Systems of A and B integrate on successful computation of the generated query from either side. Fig. 2(b) shows the centralized approach of sharing health data between four healthcare units. The data is centrally stored and no individual communication is allowed between any units. The request is centrally received and handled accordingly. The control lies at single point and usually managed by a single authority. Fig. 2(c) points towards decentralized approach where certainty of possible sharing between hospitals A and B is quite low as opposed to much systematic layered-approach. Sharing depends upon the prevalent interoperability between A and B. The request is made and the compatibility is checked on both sides and if possible, the hospitals are allowed the access to the data storage of each other. Fig. 2(d) refers to the similarity approach where the policies of A and B are reframed and refined on receiving the query. The similarity analyser generates a security level and modifies the policies of A and B. The request is then made and solution provided based on the compatibility of security levels assigned by the analyser. This approach utilizes the advantages of the previous approaches providing a more dynamic and robust solution to the discussed problem. On the other side, heterogeneity of data and environment increases the complexity of this approach.

3.1 Achieving Interoperability and Security of EHR

The advantages and disadvantages of each approach are viewed with respect to interoperability and security of EHR. Layered approach is based on the classification of inputs into syntax, object and semantic attributes. Decomposition of task gives ease in functionality and reduces complexity of execution. The functionality of each layer is independent of other. Hence, mapping is required between layers to generate a consolidated output or decision on the given input size. It is a viable approach in achieving interoperability but needs to address integrity issues while sharing EHR across multi-platform environments. Centralized approach manages and controls sharing of EHR in flexible client-server environment. Interoperability can be achieved well if the collaborating units are kept to minimum. With the increase in the number of units interoperability becomes highly complex and due to the flexible nature of the approach, sensitive health data becomes highly vulnerable to security breaches. Decentralized approach exhibit high security because no direct access is permitted to each other databases. The organizations obtain the permit to share the data explicitly and only after gaining permission can access each other's data. Though, highly robust security parameter, decentralized approach falls low on interoperability as no EHR-system mutually

integrates its functionality with other. Hence, each system has its own set of policies and rules implemented on individually set schemas and languages. Vast IT techniques create a jargon of disparity in such systems resulting in low interoperability. Similarity-based approach is a two-step process. Firstly, security level is assigned to each user in the organizational hierarchy and then linearly matched with the security levels of other organization. The data is shared if the similarity exists between the users and resource security levels in the requested query. The approach maintains a balance between interoperability and security of EHR while sharing between independent healthcare users.

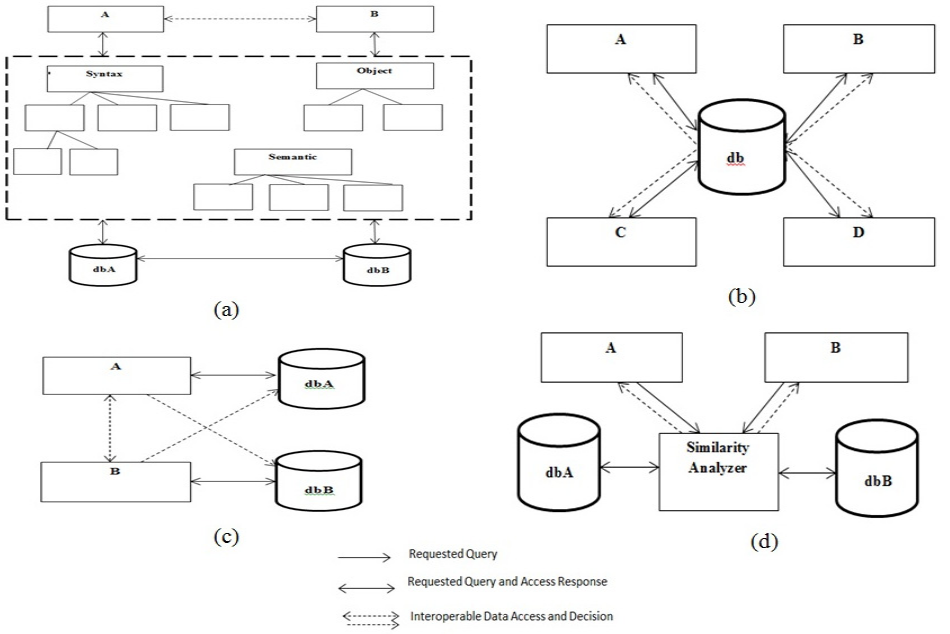

Fig.2. Achieving interoperable sharing of health data: (a) Layered Approach (b) Centralized Approach (c) Decentralized Approach (d) Similarity Approach

4. Issues to Syntactic and Semantic Interoperability

In healthcare domain, semantic interoperability[16] is most needed when there is need to combine and share Electronic Health Records from different systems. To gain the maximum benefits of information technology, full semantic interoperability is required across heterogeneous EHR system. It will provide requisite input to decision support, workflow management and evidence based healthcare. Some of the issues that need to be addressed while achieving complete interoperability and acceptable security of sharable EHR-systems are stated as under.

- *Partial Mappings from Multiple Sources:* Integrating the attributes defined in multiple systems often result in semantic differences leading to partial mapping of data[17]. This happens due to incompatible or non-formalized structuring of data.
- *Need of User Intervention:* Identifying commonalities of meaning and usage of conflicting terms in health data is impossible without user intervention. Conflicts often lead to undue disclosure of data. Hence, designing a pure dynamic framework for sharing data embedding semantic dissimilarities is a herculean task.
- *Setting of Standards/Guidelines:* It is necessary to analyse and classify policy-conflicts in order to establish a set of principles that ensure the modified rule is syntactically and/or semantically valid.
- *Addressing Contextual Constraints:* Can establish a list of vocabulary but identifying the correct interpretation of similar term having different meanings still remains a challenge. To introduce constraints

brought about by context requires an enormous repository of word meanings of medical terms that can be used to determine the semantic relationships between one attribute value and another.

- *Existence of Semantic Differences in Attributes:* The semantic differences in attributes[11] need to be identified with the help of reasoning rules that would form the basis for logically establishing similarities between them. This is a problem that can be best resolved through natural language processing techniques. In machine translation systems, it is well known that the translation pattern pairs of source and target language are effective in interpreting the correct meaning.
- *Platforms for Semantic Interoperability:* Use of information retrieval techniques and artificial intelligence to evaluate the profile similarity of different elements in a vector space model.
- *Ontology Mapping:* Ontology mapping[18] to search for a global optimal solution that best suites the ontology constraints can be best achieved through exploration of non-instance based learning approach. Ontology mapping relies heavily on features of its concepts definitions and explicit semantics of these definitions. Ontology mapping is a successful technique for information retrieval but is quite subjective.
- *Interpreting Medical Terminologies:* Understanding and interpreting medical terminologies[9] correctly is a bigger challenge. The art of deciphering the semantic dissimilarities prevalent in interoperable structures using knowledge management techniques is one of the viable solutions.

The above mentioned interoperability issues affect the confidentiality, integrity and availability of data. The sensitive and confidential data becomes vulnerable to not only external but also internal breaches.

5. Conclusion

Achieving semantic interoperability requires user intervention and thus limits the possibility of controlling and managing secured sharing of EHRs dynamically. Syntactic interoperability on the other hand has low-level technical issues like that of formats, schema and protocols that can be resolved using various techniques and approaches. Semantic interoperability requires different levels of integration in inter as well as intra organizations and is difficult to obtain. Also, it is observed that healthcare domain exhibits data having high sensitivity in terms of required security. Moreover, the need of EHR security differs from person to person or case to case. Hence, a dynamic and robust technique or approach must be appropriately selected for permitting secured sharing of sensitive health data in disparate interoperable healthcare domain.

References

1. IEEE, Standards glossary, 2013. In IEEE Retrieved from http://www.ieee.org/education_careers/education/standards/standards_glossary.html
2. Young, P., Chaki, N., Berzins, V. and Luqi, Evaluation of middleware architectures in achieving system interoperability, Rapid Systems Prototyping Proceedings, 14th IEEE International Workshop 2003; p. 108-116
3. ISO/TR 20514:2005, Health informatics -- Electronic health record -- Definition, scope and context by ISO/TC 215, Multiple. Distributed through American National Standards Institute, 2007; p. 1-27
4. Hovenga, E.J.S., Health Information Governance in a Digital Environment, Grain, H (eds.), IoS Press, 2013; 193: p. 1-384
5. Rules and Regulations, Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164, Modifications to the HIPAA Rules, Final Rule 2013, Federal Register, 2013;78: p. 1-17
6. NIST, Guide for Mapping Types of Information and Information Systems to Security Categories, National Institute of Standards and Technology (NIST), NIST Special Publication 800-122, 2010; p. 1-59
7. World Health Organization, Electronic Health Records: Manual for Developing Countries, 2006.
8. Perumal T., Ramli A.R., Leong C.Y., Mansor S. and Samsudin K., Interoperability for Smart Home Environment Using Web Services. International Journal of Smart Home. 2008;2(4).
9. Bhartiya, S. and Mehrotra, D., Threats and Challenges to Security of Electronic Health Records. In Proc. of QSHINE 2013, Social Informatics and Telecommunications Engineering, LNICST, 2013; 115: p. 543–559
10. George, A.T. and Michael P. Interoperability among Heterogeneous Services. International Journal of Web Services Research, Zhang Liang-Jie, T.J. IBM eds., 2008; 5(4): p. 79-110.
11. Dolin, R. H. and Alschuler, L., Approaching semantic interoperability in Health Level Seven, J Am Med Inform Assoc., 2011;18(1): p.99-103
12. Mao, M., Ontology Mapping: Towards Semantic Interoperability in Distributed and Heterogeneous Environments, ProQuest, 2008; p.1-163
13. Melnik, S., and Decker S., A Layered Approach to Information Modeling and Interoperability on the Web, In Proceeding of the ECDL'00 Workshop on the Semantics Web, 2000. Retrieved from http://www-db.stanford.edu/~melnik/pub/sw0

14. Carmagnola, F., Cena, F.,: From interoperable user models to interoperable user modeling, Proceedings of the 4th international conference on Adaptive Hypermedia and Adaptive Web-Based Systems, Dublin, Ireland, 2006
15. Bhartiya S. and Mehrotra D.: An Access Control Framework for Secured Sharing of Electronic Health Records using Hierarchy Similarity Analyzer, Int. J. of Electronic Healthcare, Inderscience, 2015;8(1): p. 25-50
16. Hwang, KH, Chung, Kyo-IL, Chung, M-Ae., Choi, D., Review of Semantically Interoperable Electronic Health Records for Ubiqu-103itous Healthcare, Healthc Inform Res. 2010; 16(1): 1–5.
17. Harvey,F., Kuhn,W., Pundt, H., Bishr, Y., Riedemann, C. Semantic interoperability: A central issue for sharing geographic information, The Annals of Regional Science, 1999; 33(2): p. 213-23
18. Kalfoglou, Y., Schorlemmer, M., IF-Map: An Ontology-Mapping Method Based on Information-Flow Theory, S. Spaccapietra et al. (Eds.): Journal on Data Semantics, LNCS 2800, Springer-Verlag Berlin Heidelberg 2003; p. 98-127