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.

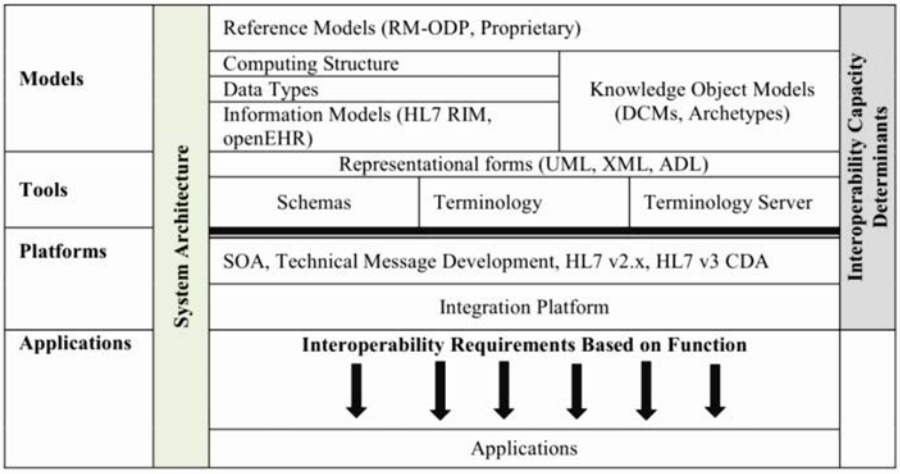

Fig.1. Architecture of Interoperable EHR-Systems[4]

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