Family Medicine & Medical Science Research

Editorial Open Access

Interoperability and Security Challenges in e-Health Systems

Nabil A Alrajeh*

Department of Biomedical Technology, College of Applied Medical Sciences, Saudi Arabia

Introduction

The health system is the culmination of organizations, institutions, and resources which work together for the purpose of providing health care and improvement in health. This complex system comprises a number of different levels: patient, practitioner, Care Team, Care Delivery Institutions and Global Environment.

Over the last decade, the need to develop and organize new ways of providing efficient health-care services has been accompanied by major advances in information technology, and particularly by the ability to record easily and inexpensively, information about every health transaction and to access this information instantly no matter where it is stored. This has resulted in a significant growing of interest in and recognition of the importance of health information technology (e-Health), and the mobilization of health information electronically by mainly building strong and efficient Healthcare Collaboration Network (HCN) established for coordinating the information and services delivery in healthcare ecosystems.

Therefore, two main trends have to be taken into account when developing e-Health systems: (i) to ensure the interoperability enabling the healthcare institutions cooperation and allowing the sharing of clinical data across disparate applications and systems; (ii) and to implement appropriate security safeguards protecting electronic healthcare information that may be at risk.

Service Based Healthcare Collaboration Network Interoperability

The reasons for exchanging data and invoking authorized partners services are many and varied in Healthcare domain, including: (i) Informing the patient of care decisions, (ii) Following up quality of care, (iii) Determining if treatments are necessary and reasonable for the purposes of making payments, (iv) Responding to healthcare emergencies such as public health threats, (v) Performing studies of population health, (vi) Conducting research into the effectiveness of existing and emerging treatment mechanisms [1].

If interoperability is a challenge in the IT domain, this issue gets more challenging in HCN since clinical information is both critical and complex. There are many approaches to effectively establish interoperability across a HCN. We can mention among others: (i) Healthcare information standards, unified approach suggesting the compliance of healthcare information systems with a set of commonly accepted data representation and communication standards [2]; (ii) Adoption of a unique "fully integrated" systems, using fully integrated information systems by a single vendor [3]; (iii) Custom interfacing for data exchange, aiming at the development of point-to-point custom interfaces between information subsystems [2-4]; (iv) Process Composition, dealing with collaboration among healthcare processes by linking the underlying sub supporting systems responsible for executing the corresponding sub processes within each HCN member [2].

In addition to the information exchange issues, there is a need for service integration and application reuse. This refers to the concept that healthcare information systems should be able not only to access and use services provided by others but also to re-use their functionality. Thus, it is theoretically possible to build complex information services from the composition of existing ones. In this perspective, Service oriented architecture (SOA) [5] and the supporting Web Services (WS) [6] technology have an important role to play.

Indeed, the service oriented interaction approach holds promise to create HCN that are interoperable, composable, extensible, and dynamically reconfigurable. This federated approach is used to establish new composite Transversal Healthcare Business Process across HCN. It reuses existing services within entities to provide added value patient-centered services.

Standard Based Healthcare Information System Security

The rise in the adoption rate of ICT creates an increase in potential security risks and therefore, all healthcare organizations have to deal with the protection of the confidentiality, integrity and security of healthcare information existing whether in clinical applications, databases, storage infrastructure or patient portals. Security threats if left unchecked can jeopardize the confidentiality, integrity and availability of individual and private information and in the end may result in untold damage to the all healthcare stakeholders. To sum up, keeping health information private and secure, while ensuring appropriate access, is essential to consumer trust and the success of their efforts to promote better quality healthcare [7].

Thus, healthcare organizations must put in place policies and controls (e.g. data, access and compliance controls) to protect it from security risks as it travels throughout the infrastructure, and ensure that the whole lifecycle of healthcare information protection and security is auditable. Numerous standards and guidelines are dedicated to HIS Security, such as: the European legal framework 95/46/EC [8] targeting the harmonization of European countries regulations related to individual data protection and circulation; the European project SEISMED (Secure Environment for Information Systems in Medicine) guidelines for security taking into account the principles of health care data processing and the various legislations within the EU [9]; the BMA (British Medical Association) security policy [10] focussing on access control and the management of medical records;; and the Health Insurance Portability and Accountability Act (HIPAA) law established in the USA specific for the development of security national standards for HIS[11].

HIPAA goal is to protect patients' rights and privileges [12], and its enactment seeks to simplify and encourage the electronic transfer of information by replacing many of the current nationally used non-standard formats with a single set of electronic transactions that would be used throughout the health care industry [13]. In this vein, the Act calls for simplification of administrative procedures and mandates health care organizations to implement standard formats for all transactions. HIPAA regulations are divided into four Standards or Rules: (i) Privacy, (ii) Security, (iii) Identifiers, and (iv) Transactions and Code Sets.

HIPAA security rules are based on the following principle: a person

***Corresponding author:** Dr. Nabil A Alrajeh, Department of Biomedical Technology, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia P.O. Box 91138, Tel: +966505268838; E-mail: nabil@ksu.edu.sa

Received November 20, 2012; **Accepted** November 21, 2012; **Published** November 23, 2012

Citation: Alrajeh NA (2012) Interoperability and Security Challenges in e-Health Systems. Family Med Medical Sci Res 1:e103. doi:10.4172/2327-4972.1000e103 who maintains or transmits health information is required to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of that information. These safeguard categories are divided into standards and implementation specifications that provide instructions for putting in place the components -- notably in the form of policies and procedures of the three categories.

Two main reasons can be mentioned for the adoption and/or the adaptation of HIPAA as a global framework for the HIS Security Qualitative Assessment: (i) The basic safeguards to implement are clear and well defined. This can help strongly to list all the inquiries and observations to make during the HIS Security Qualitative Assessment; and (ii) Despite the fact HIPAA standards are obligatory only for the USA; they have influenced the development and operation of healthcare information systems world-wide [14].

References

1. Oguejiofor E, Cunico H, Franck R, Yuan L, Lopriore P, et al. (2006) Healthcare Collaborative Network, Solution Planning and Implementation. IBM RedBook Report.
2. Dadam P, Reichert M, Rinderle S, Jurisch M, Acker H, et al. (2008) Towards truly flexible and adaptive process-aware information systems. Lecture Notes in Business Information Processing 5: 72-83.
3. Littlejohns P, Wyatt JC, Garvican L (2003) Evaluating computerised health information systems: hard lessons still to be learnt. BMJ 326: 860-863.
4. Apostolakis I, Valsamos P (2007) A Healthcare Interoperability Framework Based on the Composition of Semantic Web Services. The Journal on Information Technology in Healthcare 5: 123–130.
5. OASIS “Reference Model for Service Oriented Architecture 1.0” OASIS Standard, 12 October 2006. http://docs.oasis-open.org/soa-rm/v1.0/
6. W3C “Web Services Architecture” W3C Working Group Note 11 February 2004. http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/
7. Improving the quality of healthcare through health information exchange. Selected findings from e health initiative’S (2006) Third annual survey of health information exchange activities at the state, regional and local levels. Washington, D.C.
8. Directive 95/46/CE du Parlement Européen, adoptée par le Conseil Européen le 24 Juillet 1995 “On the protection of individuals with regard to the processing of personnal data and on the free movement of such data, 1995.”
9. Barber B, Bleumer G, Davey J, Louwerse K (1995) How to achieve secure environments for information systems in medicine. Medinfo 8: 635-639.
10. British Medical Association. Security in Clinical Information Systems. BMA, London- ISBN 0-7279-1048-5, 1996.
11. HIPAA Security Series: 1-Security 101 for Covered Entities, 2-Security Standards Administrative Safeguards, 3-Security Standards Physical Safeguards, 4-Security Standards Technical Safeguards, 5-Security Standards Organizational, Policies & Procedures, and Documentation Requirements” CMS – Centers for Medicaire & Medicaid Services, 2007.
12. Choi YB, Capitan KE, Krause JS, Streeper MM (2006) Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. J Med Syst 30: 57-64.
13. Chung K, Chung D, Joo Y (2006) Overview of administrative simplification provisions of HIPAA. J Med Syst 30: 51-55.
14. S. Kokolakis, Lambrinoudakis C (2005) ICT Security Standards for Healthcare Applications. Upgrade 6.