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 health services within entities to provide added value patient-centered services. 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.

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] focusing 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


Copyright: © 2012 Alrajeh NA. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.
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 worldwide [14].

References