Key security and privacy issues from implementing the National Electronic Health Record in the Islamic Republic of Iran

Seyedesdigheh Seiedfarajollah ¹, Reza Safdari ¹, Marjan Ghazisaeedi ¹ and Leila Keikha ¹

¹Department of Health Information Management, School Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Islamic Republic of Iran. (Correspondence to: Leila Keikha: leilakeikha@gmail.com).

Abstract

Background: In countries that have not implemented Electronic Health Records (EHR) comprehensively, international organizations are important steps in the development of EHR.

Aims: The objective of this study was to compare different dimensions of privacy in the EHR systems for the following standards organizations: ASTM, Health Level Seven (HL7), and International Organization for Standardization (ISO), in order to create a security and privacy model for EHR.

Methods: This study was done in two steps: 1) survey of standards organizations, and 2) compare standards in comparative tables.

Results: Overall standards 12, 1 and 5 were extracted from the ASTM, HL7 and ISO respectively.

Conclusions: Evidence shows that the goal of standards was to create EHR systems that identified not only the access level of users, but taking consent for reveal information of people and also approved data by authorized persons in secure framework. In this regard, ASTM looks comprehensive to the privacy issues, while ISO18308 focuses on security issues and data interoperability simultaneously, while HL7 has emphasized access.

Keywords: Privacy, standards, confidentiality, electronic health record, informed consent

Received: 28/08/17; accepted: 04/12/17

Citation: Seiedfarajollah S; Safdari R; Ghazisaeedi M; Keikha L. Key security and privacy issues from implementing the National Electronic Health Record in the Islamic Republic of Iran. East Mediterr Health J. 2019;25(x):xxx. https://doi.org/10.26719/emhj.19.006

Copyright © World Health Organization (WHO) 2019. Some rights reserved. This work is available under the CC BY-NC-SA 3.0 IGO license (https://creativecommons.org/licenses/by-nc-sa/3.0/igo).

Introduction

In countries that either have not implemented electronic health records (EHR) comprehensively, or have had unsuccessful experiences with the implementation of EHR, utilizing the experiences of international organizations for the acceptance and incorporation of international standards are important steps in developing an EHR (1–3). However, using approved standards and modifying them according to the conditions and infrastructures of the country are key points for their successful implementation. Thus, it is necessary to assess the existing systems by current international standards and find practical solutions to close identified gaps before allocating resources.
Security and privacy are the key issues for EHR implementation systems. A literature review highlighted that technical and legal details, individual’s right to privacy and policy-making are the major challenges to the development of EHR systems in low- and middle-income countries (4–11). The objective of this paper was to study current international standards in order to create a security and privacy model for EHR. Therefore, the authors compared the different dimensions of privacy including access control, authentication / signature, consent, and security in EHR systems in the ASTM, Health Level Seven (HL7), and International Organization for Standardization (ISO). Standards 12, 1 and 5 were extracted from ASTM, HL7 and ISO respectively. Extracted standards were entered into comparison tables and evaluated in terms of number, diversity and content (Table 1).

Table 1: Guidelines of selected organizations in the field of privacy and security

<table>
<thead>
<tr>
<th>ASTM standards</th>
<th>HL7 standards</th>
<th>ISO standards</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. E1987-98*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Standard Code</td>
<td>Standard Title</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>E2084-00*</td>
<td>Standard specification for authentication of healthcare information using digital signatures.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>E2086-00*</td>
<td>Standard guide for internet and intranet healthcare security.</td>
<td></td>
</tr>
</tbody>
</table>

**Security and privacy**

According to ASTM, guidelines must be established that all patients and healthcare providers become aware of the content of their EHR. In contrast to ASTM, HL7 does not consider any guidelines in this subject, but addresses this issue through various standards with regard to the exchange of data. However, ISO’s stated key guidelines in terms of security include; validation, data integration, confidentiality and audit. In addition, ISO 18308 requirements cover legal and ethical aspects of personal information as one of the main prerequisites for the development of EHR.

**Access control**

ASTM recommends the management policy should contain licenses for authorized access. HL7 considers access control via different standards (14,15), while ISO suggests that guidelines are established to define, attach, modify and delete access to the EHR system.
Authentication / signature
According to ASTM, all data entries must be confirmed by the user identifiers. HL7 defines the vocabulary related to it and also the stated digital signature (16–18). However, according to ISO the authentication includes data source and user verification (19).

Consent
ASTM approves informed consent and recommends two types of consent; treatment and discharge consent. In HL7, the DC1.5 standard examines the creation, maintenance and verification for access to consents, licenses and advanced guides. ISO 18308 requirements also address this issue (20). Evidence suggests that Security and privacy under ASTM is approached as a comprehensive subject in security and privacy, access, electronic signature and consent issues. Moreover, ASTM has a more practical view on this by assigning category data into three categories; very restricted, restricted and usual control. HL7 has focuses on the subject of access, while ISO not only proposes requirements for security and privacy, access and consent in ISO18308, but also discusses the issue of forensic medicine and medical ethics.

Conclusion
ASTM is comprehensive with regard to the issue of privacy, but for forensic and medical ethics, ISO 18308 may be applied. Therefore, before any planning for the design and development of a national EHR, it is essential to consider the confidentiality and security subjects when examining the interoperability of data. In addition, it is important to note that such research in those countries that have not yet succeeded in implementing the EHR completely, will prevent duplication and save time and cost.

Acknowledgment
We sincerely appreciate the directors of ASTM, HL7 and ISO organizations for their cooperation with this study.

Funding: None.
Competing interests: None declared.

References