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

Seyedesedigheh Seiedfarajollah,[1] Reza Safdari,[1] Marjan Ghazisaeedi [1] and Leila Keikha [1]

[1]Department 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 in terms of 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: 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 a secure framework. In this regard, ASTM looks comprehensive for 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

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(9):656–659. https://doi.org/10.26719/emhj.19.006

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

Introduction

In countries that either have not implemented electronic health records (EHRs) comprehensively, or have had unsuccessful experiences with the implementation of EHRs, utilizing the experiences of international organizations for the acceptance and incorporation of international standards are important steps in developing EHRs (*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 EHRs 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 EHRs systems in low- and middle-income countries (*4–11*). The objective of this article was to study current international standards in order to create a security and privacy model for EHRs. Therefore, the authors compared the different dimensions of privacy including access control, authentication / signature, consent, and security in EHRs 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*).

Security and privacy

According to ASTM, guidelines must be established that all patients and health care providers become aware of the content of their EHRs. 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 EHRs.

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 EHRs 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*).

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

ASTM standards	HL7 standards	ISO standards	References
1. E1869-04 (2014) Standard guide for confidentiality, privacy, access, and data security principles for health information including electronic health records.	***1. HL7 Clinical document architecture (CDA).***	***1. ISO/IEEE 11073-10103:2014*** Health informatics – Point-of-care medical device communication – Part 10103: Nomenclature – implantable device, cardiac.	(*10,12,13*)
2. E1985 – 98 (2013) Standard guide for user authentication and authorization.		***2. ISO/TS 14441:2013*** Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment.	
3. E1714 – 07 (2013) Standard guide for properties of a universal health care identifier (UHID).		***3. ISO/TS 21547:2010*** Health informatics – security requirements for archiving of electronic health records principles.	
4. E1902-02* Standard specification for management of the confidentiality and security of dictation, transcription, and transcribed health records.		***4. ISO/TS 13606-4:2009*** Health informatics – electronic health record communication – Part 4: Security.	
5. E1986 – 09 (2013) Standard guide for information access privileges to health information.		***5. ISO/TS 17975:2015*** Health informatics – principles and data requirements for consent in the collection, use or disclosure of personal health information.	
6. E1987-98* Standard guide for individual rights regarding health information.			
7. E1988-98* Standard guide for training of persons who have access to health information.			
8. E2084-00* Standard specification for authentication of health care information using digital signatures.			
9. E2085* Standard guide on security framework for health care information.			
10. E2086-00* Standard guide for internet and intranet health care security.			
11. E2017 – 99 (2010) Standard guide for amendments to health information.			
12. E1384-07 (2013) Part 2 Standard practice for content and structure of the electronic health record (EHR).			

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 EHRs, 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 EHRs 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.

Questions essentielles concernant la sécurité et la protection de la sphère privée dans la mise en place du dossier médical électronique national en République islamique d'Iran

Résumé

Contexte : Dans les pays qui n'ont pas mis en place le dossier médical électronique (DME) de manière généralisée, les organismes internationaux jouent un rôle important dans les étapes permettant l'instauration du DME.

Objectifs : La présente étude avait pour objectif de comparer les différentes dimensions de la protection de la sphère privée dans les systèmes de DME dans les organismes de normalisation suivants : ASTM, Health Level Seven (HL7), et l'Organisation internationale de normalisation (ISO), afin de créer un modèle de sécurité et de protection de la sphère privée pour le DME.

Méthodes : La présente étude s'est déroulée en deux étapes : 1) enquête sur les organismes de normalisation, et 2) comparaison des normes à l'aide de tableaux comparatifs.

Résultats : Les normes, 12, 1 et 5 ont été extraites des systèmes ASTM, HL7 et ISO respectivement.

Conclusions : Les données montrent que l'objectif des normes était de créer des systèmes de DME qui permettent d'identifier non seulement le niveau d'accès des utilisateurs, mais aussi d'exiger l'accord des personnes pour divulguer des informations personnelles et également d'approuver les données par les personnes autorisées dans un cadre sécurisé. À cet égard, ASTM semble offrir une solution exhaustive sur les questions de protection de la sphère privée, tandis que la norme ISO18308 met l'accent sur les questions de sécurité et d'interopérabilité des données simultanément et que HL7 privilégie l'accès.

المسائل الرئيسية المتعلقة بالأمن والخصوصية في تنفيذ السجل الصحي الإلكتروني الوطني في جمهورية إيران الإسلامية

سيدي صديق سيد فرج الله، رضا صفدري، مرجان غازي سعيدي، ليلى كيخا

الخلاصة

الخلفية: في البلدان التي لم تُطبق السجل الصحي الإلكتروني تطبيقاً شاملاً، تُعتبر معايير المنظمات الدولية خطوات مهمة في سبيل تطوير سجل صحي إلكتروني.

الأهداف: تقارن هذه الدراسة بين شتَّى أبعاد الخصوصية في أنظمة التسجيل الصحي الإلكتروني وفقًا لمعايير المنظمات التالية: الجمعية الأمريكية للاختبار والمواد (ASTM)، والمستوى الصحي السابع (HL٧)، والمنظمة الدولية للتوحيد القياسي (ISO)، من أجل وضع نموذجٍ يمتاز بالأمان والخصوصية للتسجيل الصحي الإلكتروني.

طرق البحث: أُجريت هذه الدراسة في خطوتين: الأولي: لمسح معايير المنظمات؛ والثانية: للمقارنة بين المعايير في جداول مقارنة.

النتائج: استُخلصت المعايير ١٢ و١ و٥ من معايير ASTM و HL٧و ISOعلى التوالي.

الاستنتاجات: تشير الأدلة إلى أن الهدف من المعايير يتمثَّل في إنشاء أنظمة سجل صحي إلكتروني لا تحدد مستوى قدرة المستخدمين على الوصول إلى البيانات وحسب، بل تتناول أيضاً الحصول على موافقة للكشف عن معلومات الأشخاص، وكذلك البيانات المعتمدة من قِبَل أشخاص مصرَّح لهم في إطار عمل آمن. ويبدو، في هذا الصدد، أن نظام ASTM يشمل مسائل الخصوصية، بينما يركز نظام ISO ١٨٣٠٨ على مسائل الأمان وقابلية التشغيل البيني للبيانات في وقت واحد، ويشدد نظام Hl٧ على مستوى الوصول للبيانات.

References

1. Deutsch E, Duftschmid G, Dorda W. Critical areas of national electronic health record programs—Is our focus correct? Int J Med Inform. 2010 Mar;79(3):211-22. https://doi.org/10.1016/j.ijmedinf.2009.12.002

2. Sinha PK, Sunder G, Bendale P, Mantri M, Dande A. Electronic health record: standards, coding systems, frameworks, and infrastructures: John Wiley & Sons; 2012.

3. Jahanbakhsh M, Rabiei R, Asadi F, Moghaddasi H. Electronic health record architecture: a systematic review. J Paramed Sciences. 2016;7(3):29-36.

4. Dunlop L. Electronic health records: interoperability challenges patients' right to privacy. Shidler JL Com & Tech. 2006; 3:1.

5. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013 Jun;46(3):541-62. https://doi.org/10.1016/j.jbi.2012.12.003

6. Garde S, Knaup P, Hovenga EJ, Heard S. Towards Semantic Interoperability for Electronic Health Records. Methods Inf Med. 2007;46(3):332-43

7. McGinn CA, Grenier S, Duplantie J, Shaw N, Sicotte C, Mathieu L, et al. Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: a systematic review. BMC Med. 2011 Apr 28;9:46. https://doi.org/10.1186/1741-7015-9-46

8. Terry NP, Francis LP. Ensuring the privacy and confidentiality of electronic health records. University of Illinois Law Review, 2007(2):681-735

9. Fraser H, Biondich P, Moodley D, Choi S, Mamlin B, Szolovits P. Implementing electronic medical record systems in developing countries. Inform Prim Care. 2005;13(2):83-95

10. Xu W, Guan Z, Cao H, Zhang H, Lu M, Li T. Analysis and evaluation of the electronic health record standard in China: a comparison with the American national standard ASTM E 1384. International Journal of Medical Informatics. 2011;80(8):555-61.

11. Hiller J, McMullen MS, Chumney WM, Baumer DL. Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. BUJ Sci & Tech L. 2011;17:1.

12. Kwak YS. Electronic health record: definition, categories and standards. J Korean Soc Med Inform. 2005 Mar;11(1):1-15

13. ASTM. American society for testing materials 2017 (https://www.astm.org).

14. Ueckert FK, Prokosch H-U, (eds). Implementing security and access control mechanisms for an electronic healthcare record. Proceedings of the AMIA Symposium; 2002: American Medical Informatics Association.

15. Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform. 2004 Mar 31;73(3):251-7 https://doi.org/10.1016/j.ijmedinf.2003.11.018

16. Quinsey CA. Using HL7 standards to evaluate an EHR. Journal of AHIMA. 2006;77(4A):C.

17. Rau HH, Hsu C-Y, Lee YL, Chen W, Jian WS. Developing electronic health records in Taiwan. IT Professional. 2010;12(2):17-25

18. Blobel B. Security requirements and solutions in distributed electronic health records. Information Security in Research and Business: Springer; 1997:377-90.

19. Pharow P, Blobel B. Security Infrastructure Services for. Medical and Care Compunetics 1. 2004;103:434.

20. Namli T. Security, privacy, identity and patient consent management across healthcare enterprises in integrated healthcare enterprises (IHE) cross enterprise document sharing (xds) affinity domain: Middle East Technical University; 2007.