JMSR
Journal of Medical and Surgical Research

Review

ISSN: 2351-8200

JMSR 2018, Vol V; N°2: 551- 554

CONFIDENTIALITY IN ELECTRONIC HEALTH RECORDS SYSTEMS: -A REVIEW-

Assiya El Kettani, Samy Housban, Zineb Serhier, Mohammed Bennani Othmani
Laboratory of Medical Informatics, Faculty of Medicine and Pharmacy, Hassan IId University, Casablanca.

ABSTRACT

Confidentiality in Electronic Health Records systems (EHRs) entails that only authorized users can access information. It is related to transmission and storage security, but also proper authorization so that users can only access information they need to access. It is considered as one of the main concerns in implementing digital health records, in order to ensure continuity of care records and coordination between caregivers. This work focuses on listing and discussing legal issues and standards in health informatics security, data protection technics, access control methods and rights to access to data in EHRs. It also gives an overview of the Moroccan legislation on automatic processing of health data**.** These confidentiality sides should be considered to develop a safe efficient standard-based model of management of access to data, considering social and cultural factors. However, there are still challenges in making EHRs accessible to patients and the lack of common standards worldwide still constitute a barrier for an inter-organizational security.

Keywords: Confidentiality- Electronic health records- Information system

Corresponding Author:
Dr. Assiya El Kettani, **MD**.
Address: Medical Informatics Lab, Faculty of Medicine and Pharmacy, Hassan IId University, Casablanca, Morocco.
E-mail: assiyaelkettani@gmail.com

INTRODUCTION:

An Electronic Health Records system (EHRs) is an information system that helps to collect individuals' health information from birth to death so that they can be registered, and shared in different places by healthcare providers. [1] The main goal of implementing EHRs is improving the quality of care by providing an effective mean of coordination between caregivers, reducing costs, supporting provider decision making, reducing medical errors and the promotion of evidence-based medicine [2,3,4]. But in order to achieve these benefits, EHR systems need to satisfy some requirements related to data completeness, resilience to failure and the consistency of security policies [5]. The three fundamental security goals are confidentiality, integrity and availability (CIA Triad) [6]. Confidentiality entails that only authorized individuals can access information. This requires transmission, storage security and proper authorizations, so that users can only access information they need to access. Integrity requires that information is protected against unauthorized modification as well as accidental or undesired changes by authorized users. Availability is related to up-to-datedness, so that updates are almost instantaneously disseminated to all affected users. Security in health informatics also involves accountability/non-repudiation that ensures that accesses and uses of information are attributed to the corresponding party and that such actions cannot be denied afterwards [7]. This work focuses on defining legal frameworks and technical protocols of confidentiality in EHRs and overview the Moroccan legislation on automatic processing of health data.

LEGAL ISSUES AND STANDARDS IN HEALTH INFORMATICS SECURITY

Legal issues in health informatics security include: Legal aspects of medical and professional secret, rules on the automatic processing of personal data, rules on patients access to their health data, statements to do with organisms (e.g. CNIL in France), security and collaboration work in health, Telemedicine, data security technologies, home health technologies and autonomy [8].

These aspects are organized in standards that summarize clearly and concisely, in a structured manner the relevant sides of security and privacy process in order to ensure cost-effectiveness and risks prevention [9]. The most important standards are:

- The HIPAA (Health Insurance Portability and Accountability Act (US), 1996): A federal law that protects patient information and regulates patients' access to their own medical records.
- European Union (EU) Data Protection Directive 95/46/EC: A directive that regulate the protection of the processing of personal data and the free movement of this data. It is applied to personal data privacy in general, and is therefore applied to EHR data.
- Role Based Access Control Standard of the ''American National Standard for Information Technology'': A model of management of access control. [10]

ACCESS CONTROL

Access control is one of the main safeguards against improper data access. It aims to control data use of authorized users

- **User authentication systems**:

Username or identities (ID) with an associated password are the most common. However, passwords can be copied, shared or cracked by using debuggers and disassemblers. Thus, in addition to the password, there should be some other mechanisms to enhance information security. Two of the following three methods are recommended for inclusion in an identification system: ''something a person knows'' such as a login ID, email address, PIN; ''something a person has'' such as a key, swipe card, access card, digital certificate; or ''something that identifies a person'' such as biometrics (face and voice pattern identification, retinal pattern analysis, hand characteristics or automated fingerprint analysis based on pattern recognition). The insertion of an RFID (Radio Frequency Identification) chip is an invasive identification mechanism, but it can be also used for securing health information.

- **Data authentication: digital signature scheme**

It includes two procedures: the signing of data and checking the signature. Generally, public key algorithms are used. [10]

Role Based Access Control (RBAC) model is the most used to access HER. It can manage access control by an access based on the role of each user in the provision of patient care. It allows access privileges of each staff person and ensures that only authorized health care providers can access patients' health information. Administrative staff is restricted to basic information such as address, date of birth and other demographic information. RBAC can be an effective tool to manage complex role hierarchies in healthcare organizations. [11, 12]

ACCESS RIGHTS

The adoption of continuity of care records standards support data-sharing among providers and various healthcare organizations. But this will not be unless patients consent; the patient must grant access permissions and access is granted by health professionals to others (after having the patient's consent) there are:

- Implied consent (the patient consents to predefined rules unless otherwise indication)
- Express consent (the patient refuses the access unless he grants it)

Policies should regulate 4 types of access: allowed access, denied access, expected exceptions, unexpected exceptions.

In emergency situations, the emergency authentication process includes

- Verifying the authenticity of emergency
- Authentication of the person asking for each part of the process [10]

But when records are shared there are varying physicians' expectations of what data should be shared for access, the issue of who controls the data remains a problem. A minority of physicians agree that patients should control what physicians see in their record. Other questions surrounding patients' access implications of shared custodianship of information (eg. defining legal responsibility) require more exploration.

In addition to this, there is still no agreement on whether patients' entire or partial health experiences should be accessible to them and around timely access. Policies must be created to address why certain information might be excluded from patient access. [13].

DATA PROTECTION TECHNICS:

- **De-identification** is the process of removing (or modifying) identifiers from personal health data so that identification is not reasonably possible. This technic is used to prevent the misuse of health data.
- **Pseudonymisation** consists of transforming and then replacing personal data with a pseudonym that cannot be associated with the identification data without knowing a certain secret. [8,14]
- **Encryption algorithms**:

  Encryption is the process of encoding information in such a way that only authorized users can read it. EHRs should encrypt patient data in order to protect data if hardware is stolen, or messages are intercepted [15]. There are:

- Symmetric key encryptions (the encryption and decryption keys are the same) ex: AES (Advanced Encryption Standard).

- Public key systems: the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read. [8]

CLOUD COMPUTING

Cloud Computing are the latest technological trends. They provide a strong infrastructure for Health Informatics systems services over the Internet. Cloud Computing can be defined as “A computing paradigm which is a pool of abstracted, virtualized, dynamically scalable, managing, computing, power storage platforms and services for on demand delivery over the Internet”. They have opened an opportunity for healthcare organization to share part of the data with others such as government agencies, other healthcare providers, insurance companies [16, 17].

The common solution for data confidentiality in cloud computing is data encryption, as the cloud computing environment involves a large amount of data transmission, storage and handling. It needs to consider processing speed and computational efficiency of encrypting a large amount of data when choosing the type of encryption. [18]

OVERVIEW OF THE MOROCCAN LEGISLATION ON AUTOMATIC PROCESSING OF HEALTH DATA

In Morocco, the respect of fundamental rights and freedoms of individuals in relation with the processing of personal data (and therefore health data) is ensured by The National Commission for Personal Data Protection (CNDP). It was created in 2009 after adopting the Act n°09-08:

"Informatics is at the service of the citizen ... They must not compromise the identity, rights, collective and individual freedoms of the man ..."

Article I, Act 09-08, February 18, 2009 (BO No 5714 of 05- 03- 2009)

This Act was afterwards headed by the Article 24 of the Constitution of Morocco:

"Everyone has the right to protection of his private life"

Article 24 of the Constitution of Morocco 2011

According to this,

- Personal data are defined by any information, of whatever nature and regardless of the method, including sound and image, related to an identified or identifiable natural person.
- And Treatment by any operation or set of operations, carried out or not, using automatic processes and applied to personal data.

“Dahir No. 1-09-15 of 22 Safar 1430 (18 February 2009) promulgating Act No. 09-08 on the protection of individuals towards the processing of personal data”

The statements of personal data treatment to the “CNDP” are mandatory.

The Commission's missions can be summarized in five main areas:

- Information and awareness
- Council and proposal
- Protection
- Control and investigations
- Legal and technological monitoring. [19]

Later, on January 30, 2013, at the 1160th meeting of the Ministers' Deputies, Morocco has been invited to accede to the Convention (ETS No. 108) of the European Council on the protection of personal data. [20]

CONCLUSION:

Creating a useful EHRs permitting continuity of care records and coordination between caregivers requires the expertise of physicians, technology professionals, ethicists, administrative staff and patients. Although EHRs offer many significant benefits, their risks must be recognized and managed properly. Confidentiality is considered as one of the main concerns in implementing digital health records. This work may provide a list of components that should be considered in order to develop a safe efficient standard-based model of the management of access to data, considering social and cultural factors. However, there are still challenges in making electronic health records accessible to patients. And the lack of harmonized policies and common standards worldwide still constitute a barrier for an inter-organizational security.

CONFLICTS OF INTEREST: None

REFERENCES:

1. Ahmadi M, Rezaee P, Shahmoradi L. Electronic Health Records: Structure, Content and Evaluation. Tehran, Iran: Jafari; 2008.
2. Goetz Goldberg D, Kuzel AJ, Feng LB, DeShazo JP, Love LE. EHRs in Primary Care Practices: Benefits, Challenges and Successful Strategies. Am J Manag Care. 2012 Feb 1;18 (2):e48-54.
3. Bell B, Thornton K. From promise to reality achieving the value of an EHR. Healthc Financ Manage. 2011 Feb; 65(2):50-6.
4. Fowler SA, Yaeger LH, Yu F, Doerhoff D, Schoening P, Kelly B. Electronic health record: integrating evidence-based information at the point of clinical decision making. J Med Libr Assoc. 2014 Jan; 102(1): 52–55.
5. Allard T, Anciaux N, Bouganim L, Guo Y, Folgoc LL, Nguyen B et al. Secure personal data servers: a vision paper. PVLDB journal. 2010 ; 3 (1): 25-35
6. National Institute of Standards and Technology Computer Security Division. An Introduction to Computer Security: The NIST Handbook. U.S. Department of Commerce. Gaithersburg, MD: NIST; 1995:5.
7. Dehling T, Sunyaev A. Information Security and Privacy of Patient-Centered Health IT Services: What needs to be done? 47th Hawaii International Conference on System Science 2014 (HICSS '14). IEEE Computer Society, Washington, DC, USA, 2984-2993.
8. Venot A, Burgun A, Qunatin C. Informatique Médicale, e-Santé - Fondements et applications. France Springer-Verlag, 2013. http://www.springer.com/us/book/9782817803371.
9. Bouhaddou O, Cromwell T, Davis M, Maulden S, Hsing N, Carlson D et al. Translating standards into practice. Experience and lessons learned at the Department of Veterans Affairs. J Biomed Inform. 2012 Aug;45(4):813-23
10. 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.
11. Fiza A R, Zuraini I, Ganthan Narayana S. Security Issues in Electronic Health Record. Open International Journal of Informatics 2013 (1): 59-68.
12. Ferraiolo D F, Sandhu R, Gavrila S, Kuhn D R, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 2001 4 (3): 224-274
13. Beard L, Schein R, Morra D, Wilson K, Keelan J. The challenges in making electronic health records accessible to patients. JAMIA 2012, 19(1): 116-120
14. Neubauer J. Heurix A. Methodology for the pseudonymization of medical data. Int J Med Inform 2011, 80 (3): 190–204
15. EFF Surveillance Self-Defense Project. What is Encryption? <https://ssd.eff.org/en/module/what-encryption>
16. Foster l, Zhao Y, Raicu L and Lu S. Cloud Computing and Grid Computing 360-Degree Compared, The Grid Computing Environments Workshop (GCE), Austin, TX, USA, 2008: 1-10.
17. AbuKhousa E, Mohamed N, and Al-Jaroodi J. E-Health Cloud: Opportunities and Challenges, Future Internet, 2012, 4 (3): 621-645.
18. Griebel L, Prokosch HU, Köpcke F, Toddenroth D, Christoph J, Leb I et al. A scoping review of cloud computing in healthcare. BMC Med Inform Decis Mak. 2015 Mar 19;15:17
19. CNDP http://www.cndp.ma/
20. AFAPDP http://www.afapdp.org/archives/1538