Data protection in shared health records: requirements and challenges

Yara Mohammad
Dr Lampros K. Stergioulas
Dr Maryati Mohd Yusof

School of information Systems, Computing & Mathematics, Brunel University, UK

Introduction

With the advent of computers and computer networks, collecting and storing all clinical information about a patient in electronic files became reality [1].

An electronic health record (EHR) system offers improved access to patient-specific information and has major benefits in terms of the quality of health care and the quality of life of clinicians in practice [2].

The internet has offered us the capability to access medical information from anywhere, anytime, transforming the patient-doctor relationship, particularly with respect to sharing decision making between patient and doctors [3].

Privacy, Confidentiality and Security

Rindfleisch distinguished among privacy, confidentiality and security in protecting health care information [4]:

- **Privacy**: The right and desire of a person to control the disclosure of personal health information.

- **Confidentiality**: The controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.

- **Security**: A collection of policies, procedures, and safeguards that help maintain the integrity and availability of information systems and control access to their contents.

Electronic health records characteristics

Fritsche et al. noted that collection of comprehensive and valid scientific medical data through EHR should be [1]:

- Easy to install and maintain thus being less expensive.
- Time-saving for the medical staff (users) in their daily work.
- Able to store all medical information (including picture etc.) in retrievable format.
- Able to provide data validation by repeated use of the data in patient care.

Electronic health records characteristics

Shortliffe and Fagan argue that there are at least four major issues that have consistently constrained the efforts to build effective health record systems [2]:

- Standards are needed in the area of clinical terminology;
- Concerns about data privacy, confidentiality, and security;
- Challenge of data entry by physicians;
- And difficulties related to integration of record systems with other information and data in healthcare settings.

Electronic health records requirements

The basic requirements of shared health records are:

- Comprehensiveness
- Confidentiality
- Accessibility
- Liability
- Authentication
- Flexibility
- Permission
- Accessibility in emergency cases
- Maintaining Integrity of the health record

Electronic health records requirements

There are some legal Issues regarding health records such as:

- Jurisdiction
- Legally valid agreements
- Legal implications of shared practice of medicine
- Patient's right to review and release their records

Achieving Privacy in Electronic health records

In some cases to protect privacy and confidentiality, EHR data must be:

- Anonymised, and
- De-identified.

Anonymisation usually involves stripping patient identifiers (name, address, social security number, hospital record number, etc.) from records or substituting a false identifier for the real identifier [5].

De-identification entails removing the specific identifiers listed in the privacy rule and determine there is no other information that may identify the individual [6].

Current and future challenges of data protection in shared health records

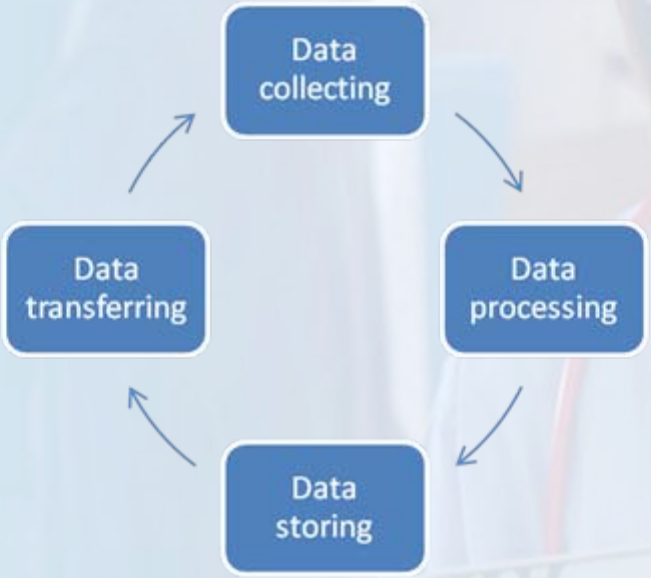
- Some patients and doctors have expressed concerns about the use of the new technology in shared health care record services. Most of these concerns are related to data protection and confidentiality issues.

- Some issues should be considered while moving from a paper-based record system to a computer-based one, such as the needed time of transmission, resources, management and administration tolls and staff, and basic technology infrastructure [2, 7].

- Some people will find ways to get secure information by exploiting human weakness to bring pressure to bear on someone with legitimate access to health information [7].

Current and future challenges of data protection in shared health records

Data could pass through four stages:



Data protection abuse could happen in any of these stages.

Conclusion

- The concept of security is intrinsically correlated with other aspects of EHR, including legal, technical, social, political and financial. The nature of these relationships between security and other issues depends on the specific user of the electronic patient records.

- The advanced technologies needed for implementing secure systems almost always make the use of the system more complex for the users. This complexity can reduce the benefits of using new technology and limit its advantages. The grand challenge for the future will be to provide a secure and at the same time user friendly electronic health record system.

References

- [1] Fritsche L, Schröter K, Lindemann G, Kunz R, Budde K, Neumayer H and Hanisch E. A Web–Based Electronic Patient Record System as a Means for Collection of Clinical Data. ISMDA. Berlin Heidelberg, 2001.
- [2] Shortliffe EH, Perreault LE, Wiederhold G and Fagan L M. Medical Informatics: Computer Applications in Health Care and Biomedicine, New York, Springer,2000.
- [3] Winker M, Flanagin A, Chi-Lum B, White J, Andrews K, Kennett R, DeAngelis C, and Musacchio R. Guidelines for Medical and Health Information Sites on the Internet, JAMA, March 22/29, Vol 283, No. 12, 2000.
- [4] Rindfleisch T. Privacy, Information Technology, and Health Care, Communications Of The Acm, August 1997/Vol. 40, No. 8, 1997.
- [5] Berman J.J. Confidentiality issues for medical data miners, Artificial Intelligence in Medicine, Volume 26, Number 1, September 2002.
- [6] HIPAA Privacy Rule, August 26, 2003. [online]. Available from http://www.wisc.edu/hipaa/ResearchGuide/deidentification.html
- [7] Mandl K, Szolovits P, Kohane I. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ, 322, 283-287, 2001.