https://doi.org/10.5272/jimab.2017232.1567

Journal of IMAB
ISSN: 1312-773X
https://www.journal-imab-bg.org

Journal of IMAB - *Annual Proceeding (Scientific Papers).* 2017 Apr-Jun;23(2):

Original article

HEALTH RECORDS AND INFORMATION TECHNOLOGY IN SUPPORT OF EXCHANGE OF HEALTH INFORMATION

Jordan Deliversky
Department of National Security, State University of Library Studies and Information Technologies, Sofia, Bulgaria.

SUMMARY:

The exchange of health information in conditions directly related to electronic environment is referred as health information technology. Usually the protection of personal health related data is comprised of various elements such as ways of information usage and access to sensitive health information.

The protection of individually identifiable health information is possible with combination of measures. Protective measures include administrative, technical and physical elements. Through such protective measures is possible to ensure confidentiality, integrity and availability of the information, while at the same time could be guaranteed the prevention of unauthorized access.

Sensitive records usually contain personal health information. Personal medical data requires high level of protection, as its content includes medical condition or diagnosis, where unauthorized access could have negative impact on one's personal and professional life.

Keywords: Electronic health record, Privacy, Access, Data protection, E-Health

INTRODUCTION

Health information in relation to new information technologies (IT) involves the exchange of health information in an electronic environment. Widespread use of health IT within the health care industry will improve the quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care. The privacy and security of health information in electronic environment must be ensured due to the fact that this information is maintained and transmitted electronically.

Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

Data protection is comprised of many elements, including where the data resides, how it is used, and who has access to it. Risk comes from both inside and outside the organization – from employees to third-party vendors and cyber criminals looking for financial gain or to intentionally or unintentionally inflict damage to an organization's reputation.

In the U.S., the federal government has recognized the advantages of health information technology. The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 requires the U.S. government to take a leadership role in developing standards by 2014 that "allow for the nationwide exchange and use of health information to improve quality and coordination of care." Under the Act, $20 billion dollars have been allocated for investment in the HIT infrastructure to encourage doctors and hospitals to electronically exchange patient health information. While the Act vigorously promotes the move to an electronically interconnected healthcare environment, it also mandates the strengthening of federal privacy and security laws to protect identifiable health information from misuse, expanding upon the regulations already in place through the Health Insurance Portability and Accountability Act (HIPAA).

The healthcare industry is held to exacting rules regarding the confidentiality of patient records. Regulations such as HIPAA, HITECH, and the EU's Data Protection Directive define guidelines around the world that the healthcare industry must adhere to in order to be compliant and protect patient privacy.

MATERIALS AND METHODS

The collection, use and disclosure of information should be guided by principles and rules, as the right to health is related to compliance with the standards and principles of human rights - universality, fairness, equality, the right to participate in decision-making, non-discrimination, transparency, etc. [1] In the regulatory framework of privacy and security attention should be paid to the collection, usage, disclosure and limitation. Limits should be set on the type and amount of information collected, used, and disclosed. Authorized persons and entities should only collect, use, and disclose information necessary to accomplish a specified purpose.

There are certain rules related to privacy and they consistent with the limitation of collection, use, and disclosure of information due to the fact that electronic health information exchange could be performed in networked environment. The privacy rule requires covered entities to limit the use, disclosure, and request of protected health

information. Such use, disclosure, and request has to be at the minimum necessary in order to accomplish the intended purpose. According to privacy regulations limits of uses and disclosure have been defined in cases where covered entities could make them without an individual's authorization. There are cases when rules on privacy include exceptions and do not require the minimum necessary standard be applied. Such exceptions are present when the disclosure of information or a request by a healthcare provider is necessary for the purpose pf treatment. Exceptions from the rule is also present when information gas been disclosure to individual who is subject to the information.

Disclosure and use of health information could be permitted in cases of public health benefit or in relation to research activities, but there needs to be maintained the appropriate balance between personal privacy interests and the public interest in regard to the relevant information. Individually identifiable information related to personal health status should be strictly protected. This protection could be accomplished with reasonable administrative, technical, and physical measures ensuring confidentiality, integrity, and availability. The aim is to prevent unauthorized or inappropriate access, use, or disclosure of sensitive information.

Safeguard requirements related to health information protection sets all forms of information, including paper, electronic and oral. Appropriate actions and relevant practices need to be accomplished when implementing technical solutions for securing possible risks.

Flexibility of safeguard standards for protection of health information does not require specific actions that have to be taken by entities, so different entities have the opportunity adequately to protect the privacy of protected health information. The type of protection applied by entities may not be the same because the circumstances may differ.

• *Electronic Health records*

An electronic health record (EHR) contents patient's individual health information in a digital version. It covers the information present of a patient's paper chart, including patient's medical history that is maintained by the healthcare provider over time. Electronic health records could contain information such as laboratory data, past medical history, radiology reports, medications, immunisations, etc.

The electronic health record could lead to improvement in patient's care via introducing the use of evidence-based tools, reduce of medical errors as well as accuracy and clarity of medical records. By providing access to health information there is visible mechanism of reducing medical costs as duplications of tests could be decreased. The reduce of delay in treatment of patients along with sufficient information could avoid delays in providing healthcare services and could improve the decision taking process for each individual patient.

Electronic health records could differ from other types of health information records, particularly from paper records as special considerations are distinguishing EHR. Different users could access an electronic version of patient's health record and this could be obtained even simultaneously. The access to EHR could be controlled by mechanisms, which are not applicable for paper records.

Regarding personal health information protection, it is important to note that health records may consist of both hard copy - usually paper and electronic health records. Handling personal health information is considerable in regard to relevant health information held in the other format. When deciding on the content of the health record it is important to make a review on the information both on the hard copy and on the electronic version of the health record. [2]

The positive aspect of electronic health record is related to real time mechanism for recording health information as records are patient-centered and make information available instantly. The information could be accessed securely prior to authorization of the user.

Electronic health record system could go beyond standard clinical data, which usually is collected in healthcare provider's office as it could offer broader view of a patient's health care. Such kind of health records could be created and managed in a digital format allowing information to be shared across health care organization. This system allows healthcare providers and organisations such as laboratories, medical facilities, pharmacies, emergency centers to share in safe environment, protecting sensitive medical data regarding each and every patient.

• *Electronic health records management*

Electronic health records management (EHRM) is the process by which electronic health records are created or received and preserved. Electronic health record usually includes information that is recorded on any electronic medium and is intended to provide documentation for long-term retention. Such information often has legal or business evidentiary value.

Electronic health records management requires decision making and planning throughout the entire life cycle of the electronic health record - from planning, processing, distribution, maintenance, storage, and retrieval of the health record to its ultimate disposition, including archiving or destruction. During the early phases of electronic health records management system development, it is important to make critical decisions if a paper copy or an electronic file will be used in order to be avoid the situation when both systems have been maintained.

Healthcare information management (HIM) ensures specific type of data to be related to the decision making process, including clinical, demographic, financial, and administrative data. Healthcare information management professionals could provide optimisation and management of electronic health record systems as they can ensure optimal management as regard to competences, knowledge and skills, because of the opportunity for information to be easily shared. [3] Advanced technologies and systems make it possible for healthcare information management practitioners to fulfill roles such as patient advocate, data translator, and public health officer.

The e-health environment encompasses much more than the storage and retrieval of information. It places new

demands on the healthcare information management professional to assist the consumer in healthcare across the continuum of care.

The e-health environment is increasing the ability of healthcare information management professionals to manage data and assist in the development of decision support systems for individual and public health data.

• *European Union perspective on electronic health records*

The definition of electronic health records contained in the Commission Recommendation of 2 July 2008 covers different types of electronic health records. According to the definition provided by the European Commission, electronic health record means a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes. [4]

Achieving and maintaining cross-border interoperability of electronic health record systems implies managing a continuous process of change and the adaptation of a multitude of elements and issues within and across electronic infrastructures in European Union Member States. Electronic infrastructures are used for exchange of information related to personal health status and it interacts aiming to ensure quality and safety of healthcare services provided to every patient individually. High quality and safety of healthcare services provided to patients is the ultimate goal.

DISCUSSION

There are major disparities between countries on the deployment of electronic health records part of an interoperable infrastructure that allows different healthcare providers to access and update health data in order to ensure the continuity of care of the patient. The same is applicable to the approach taken to regulate electronic health records, as some countries have set specific rules for electronic health records, while others rely on general health records and data protection legislation. It is essential to create an organizational framework and working process that will enable cross-border interoperability of electronic health record systems. This operational mechanism should be based on a roadmap, developed by each Member State country.

Compatibility of electronic health record systems at the technical level is the essential prerequisite for interoperable electronic health record systems. In relation to that, Member states should undertake a comprehensive survey of existing technical standards and infrastructures that may facilitate the implementation of systems supporting cross-border healthcare and the provision of healthcare services throughout the Community, especially those related to electronic health records and exchange of information.

There is a need for a mutually recognizable conformity testing procedures that are valid throughout the Community or which serve as a basis for each Member State's certification mechanism. Member states should apply properly the existing e-Health standards and profiles, namely those related to interoperability of electronic health record systems, in order to enhance users' confidence in those standards. All European union member states should ensure that the fundamental right to protection of personal data is fully and effectively protected in interoperable e-health systems, in particular in electronic health record systems, have to comply with provisions of EU protection of personal data regulatory requirements.

It is necessary to create enough reliable mechanisms for protection, which not to restrict fundamental rights and freedoms of every citizen. [5]

Processing of personal data contained in the electronic health records and their systems is particularly sensitive and therefore subject to the special data protection rules on the processing of sensitive data. Article 8 of Directive 95/46/EC prohibits in principle the processing of sensitive data concerning health. Limited exemptions to this prohibition principle are laid down in the Directive, in particular if processing is required for specified medical and healthcare purposes. Aware should be paid on the fact that interoperable electronic health record systems increase the risk that personal data concerning health could be accidentally exposed or easily distributed to unauthorised parties, by enabling greater access to a compilation of the personal data concerning health, from different sources, and throughout a lifetime. [6]

• *Bulgarian perspective on electronic health records*

Individual Personalized Information System (PIS) records exist for every person covered under the Health Insurance Law in Bulgaria. The Personalized Information System is an electronic record system set in place by the National Health Insurance Fund (NHIF). PIS records contain information on all medical care performed on a person during the last five years period of time and covered by the NHIF.

However, PIS records are created by the NHIF mainly with an informational and financial control purpose, and not as a tool to record and share electronic health data for medical purposes. There are no specific legal provisions applicable to PIS records. Therefore, general rules on health information, data protection, liability and secondary use apply to PIS records.

The NHIF has the obligation to provide to persons covered under the Health Insurance Law access to all information on medical care concerning them and performed during the last five years that enters in the "basic package" covered by the NHIF. Information provided in PIS records reaches back to 2009 with regard to medical care provided by general practitioners, medical specialists, hospitals, medical laboratories and pharmacies. Dental care information contained in PIS records only reaches back to 2012.

Bulgaria has detailed requirements applying to institutions hosting personal data. Administrators cannot begin collecting, hosting and processing personal data before being officially registered by the Commission for Personal Data Protection. The Commission controls Administrators' compliance of personal data protection require-

ments and can impose mandatory instructions on them.

Under the Health Insurance Law people can access their PIS records by using an electronic signature or a unique access code. They can also grant access to their PIS records to health practitioners on a case-by-case basis. However, only health practitioners contracted by the NHIF have the right to access PIS records by using their electronic signatures and "unique identification number", both given only to health practitioners that are members of the Bulgarian Medical Association. Therefore, health practitioners of another Member State cannot access PIS records.

The NHIF has to keep all information for 5 years after the end of their national health insurance coverage. However, there are no specific rules neither about the data from PIS records at the end of the archiving duration nor a specific obligation to destroy PIS records.

Pursuant to Article 25 of the Personal Data Protection Law, after the Administrator has achieved the purpose of personal data processing, the Administrator is obliged to destroy the data or to transfer it to another Administrator. If an Administrator wants to store data for historical, statistical or scientific purposes, the data has to be anonymised and the Administrator has to inform the Commission for Personal Data Protection.

In its current architecture, the PIS could serve as foundation for the future development of EHRs in Bulgaria. Firstly, the Integrated Information System of the NHIF offers an already existing and extensive database as all the medical care reports of all health practitioners contracted by the NHIF – individual health practitioners, hospitals, laboratories, pharmacies – are centralized in it. Moreover, this database is regularly updated, on a daily or monthly basis, by NHIF Partners who are obliged to send their medical care reports in order to receive reimbursement. [7]

CONCLUSION

Health records are among the most sensitive records available containing information concerning an individual. The unauthorized disclosure of a medical condition or diagnosis could have negative impact on individual's personal and professional life. Electronic health record systems have the potential to achieve greater quality and security of health information than traditional forms of health records. Electronic health record systems' provide easier access to health information and enhance safety and quality of healthcare services provided to patients.

REFERENCES:

1. Neikova M, Deliverska M. [Legal Aspects of mobile healthcare.] Burgas Free University, Legal articles. 2016; 23:379-384. [in Bulgarian]

2. Kierkegaard P. Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review.* 2011 Sep;25(5):507-515 [CrossRef]

3. Nguyen L, Bellucci E, Nguyen LT. Electronic health records implementation: an evaluation of information system impact and contingency factors. *Int J Med Inform.* 2014 Nov; 83(11):779-96. [PubMed] [CrossRef]

4. Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282) *OJL.* 190, 18. 7. 2008, p.37–43. [Internet]

5. Deliverska M. [Collecting, processing, storage and use of biometric data – ethical and legal aspects]. Burgas Free University, New Idea in Education. 2016; 2:68-72 [in Bulgarian]

6. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJL.* 281, 23. 11. 1995, p.31-50. [Internet]

7. Overview of the national laws on electronic health records in the EU Member States, National Report for Bulgaria, 2014. [Internet]

Please cite this article as: Deliversky J. Healt records and information technology in support of exchange of healt information. *J of IMAB.* 2017 Apr-Jun;23(2):1567-1570. DOI: https://doi.org/10.5272/jimab.2017232.1567

Received: 21/03/2017; Published online: 31/05/2017

Address for correspondence:
Jordan Deliversky, PhD
Department of National Security, State University of Library Studies and Information Technologies, Sofia.
119, Tsarigradsko Shose bvld., 1784 Sofia, Bulgaria
Mobile: +359888856073
E-mail: deliversky@yahoo.com