http://dx.doi.org/10.5272/jimab.2016222.1182

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

Journal of IMAB - *Annual Proceeding (Scientific Papers)* 2016, vol. 22, issue 2

HEALTH INFORMATION TECHNOLOGY IN EXCHANGE OF HEALTH INFORMATION

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

SUMMARY:

Health information technology involves the exchange of health information in an electronic environment. Data protection is comprised of many elements, including where the data resides, how it is used, and who has access to it.

Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized access, use, or disclosure.

Health records are among the most sensitive records available containing information concerning an individual. The unauthorized disclosure of a medical condition or diagnosis could negatively impact an individual's personal and professional life.

Keywords: Electronic health record, Privacy, Access, Data protection

Health information technology (health 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. It is imperative that the privacy and security of electronic health information be ensured as 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 c (HIPAA).

In a 2010 report by the Healthcare Information and Management Systems Society, since 2008, more than 110 healthcare organizations reported the loss of sensitive patient data affecting over 5.3 million individuals. In addition, according to the Federal Trade Commission, more than 300,000 Americans were victims of medical identity theft in 2009.

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.

The collection, use and disclosure of information should be guided by principles and rules. The Collection, Use, and Disclosure Limitation Principle in the Privacy and Security Framework emphasizes that appropriate limits should be set on the type and amount of information collected, used, and disclosed, and that authorized persons and entities should only collect, use, and disclose information necessary to accomplish a specified purpose. The Privacy Rule is consistent with the Collection, Use, and Disclosure Limitation Principle and supports adherence to the principle by covered entities that participate in electronic health information exchange in a networked environment. In particular, the Privacy Rule:

1) Generally requires covered entities to limit uses, disclosures, and requests of protected health information (PHI) to the minimum necessary; and

2) Defines and limits the uses and disclosures covered entities may make without an individual's authorization.

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The Privacy Rule also requires covered entities to take reasonable steps to limit any requests for PHI to the minimum necessary, when requesting such information from other covered entities. In some cases, the Privacy Rule does not require that the minimum necessary standard be applied, such as, for example, to disclosures to or requests by a health care provider for treat-

ment purposes, or to disclosures to the individual who is the subject of the information.

The Privacy Rule defines and limits the uses and disclosures of protected health information a covered entity may make without the individual's authorization. In doing so, and consistent with the Collection, Use, and Disclosure Limitation Principle, the Privacy Rule defines the permitted uses and disclosures based on the purpose of the use or disclosure, and attaches conditions accordingly. For example, the Privacy Rule generally permits covered entities to disclose protected health information for the core health care functions of treatment, payment for care, and health care operations, with few exceptions and limitations. In addition, in recognition of the important uses made of health information outside of the health care context, the Privacy Rule permits uses and disclosures for a number of additional public policy and benefit purposes, such as research or public health, without the individual's authorization. However, specific conditions or limitations apply to uses and disclosures by a covered entity for these purposes, to strike an appropriate balance between the individual's privacy interests and the public interest need for this information.

Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

The Privacy Rule's safeguards standard assures the privacy of protected health information by requiring covered entities to reasonably safeguard protected health information from any intentional or unintentional use or disclosure in violation of the Privacy Rule. The safeguards requirement, as with all other requirements in the Privacy Rule, establishes protections for protected health information in all forms: paper, electronic, and oral. Safeguards include such actions and practices as securing locations and equipment; implementing technical solutions to mitigate risks; and workforce training.

The Privacy Rule's safeguards standard is flexible and does not prescribe any specific practices or actions that must be taken by covered entities. This allows entities of different sizes, functions, and needs to adequately protect the privacy of PHI as appropriate to their circumstances. However, since each covered entity chooses the safeguards that best meet its individual needs, the types of protections applied may not be the same across all participants exchanging electronic health information to or through a health information organization (HIO), and some participants may not be covered entities.

· *Electronic Health records*

An electronic health record (EHR) is a digital version of a patient's paper chart. It is an electronic version of a patients medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. Electronic health records can:

– Contain a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results.

– Allow access to evidence-based tools that providers can use to make decisions about a patient's care.

– Automate and streamline provider workflow.

The electronic health record can improve patient care by:

– Reducing the incidence of medical error by improving the accuracy and clarity of medical records.

– Making the health information available, reducing duplication of tests, reducing delays in treatment, and patients well informed to take better decisions.

– Reducing medical error by improving the accuracy and clarity of medical records.

Electronic health records differ from paper health records in ways that warrant special consideration. It is possible to have a single electronic health record simultaneously accessible at multiple sites, giving more people access. It is also possible to control access to an electronic health record in ways that are not possible with a paper health record.

Health records may consist of both hard copy (paper) and electronic health records (sometimes referred to as a hybrid record). When handling personal health information, it is important to consider whether relevant health information is held in the other format and whether both the electronic health record and the hard copy health record need review when making a decision about the health information contained in the records.

Electronic health records are real-time, patient-centered records that make information available instantly and securely to authorized users. While an electronic health record does contain the medical and treatment histories of patients, an electronic health record system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care.

One of the key features of an electronic health record is that health information can be created and managed by authorized providers in a digital format capable of being shared with other providers across more than one health care organization. Electronic health records are built to share information with other health care providers and organizations – such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics – so they contain information from all clinicians involved in a patient's care.

· *Electronic health records management*

Electronic health records management (EHRM) is the process by which electronic (e.g., digital) health records are created or received and preserved for evidentiary (e.g., legal or business) purposes.

An electronic record includes information that is:

– Recorded on any electronic medium (e.g., magnetic medium)

– Intended to provide documentation for long-term retention that 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. Decision making includes, but is not limited to, what electronic health records to keep and for how long, the assignments of authorities and responsibilities, the design and administration of the process, and the audit and review of the process's performance.

In the early phases of electronic health records management system development, it is important to make critical decisions about the role and use of paper and film to avoid the dilemma of maintaining dual systems.

Healthcare information management (HIM) ensures the availability of clinical, demographic, financial, and administrative data to facilitate real time healthcare delivery and critical health - and business - related decision making for multiple purposes across diverse organizations, settings, and disciplines. Healthcare information management professionals are ideally suited to provide the healthcare entity with the necessary leadership to ensure that the electronic health record and the electronic health record system are optimally managed.

The evolution from a paper-based medical record model to an electronic health record model has opened up many avenues for healthcare information management experts to apply and share their core competencies, knowledge, and skills. 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.

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 Member States. These electronic infrastructures are necessary to exchange information, interact cooperate in order to ensure the highest possible levels of quality and safety in healthcare provision to patients.

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 can be said about the approach taken to regulate electronic health records - some countries have set specific rules for electronic health records, others rely on general health records and data protection legislation. It is essential to create an organizational framework and process that will enable cross-border interoperability of electronic health record systems. This should be based on a roadmap, developed by Member States.

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, in conformity with Community provisions on the protection of personal data.

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.

• *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 requirements and can impose mandatory instructions on them.

Under the Health Insurance Law people can access to 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 5 years after the end of one's 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.

Health records are among the most sensitive records available containing information concerning an individual. The unauthorized disclosure of a medical condition or diagnosis could negatively impact an individual's personal and professional life. Electronic health record systems have the potential to achieve greater quality and security in health information than the traditional forms of health records. Interoperability of electronic health record systems should make access easier, and enhance the quality and safety of patient care.

REFERENCES:

1. 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]

2. 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]

3. Kierkegaard P. Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review.* 2011 Sep;27(5):503-515. [CrossRef]

4. 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]

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

Please cite this article as: Deliversky J. HEALTH INFORMATION TECHNOLOGY IN EXCHANGE OF HEALTH INFORMATION. *J of IMAB.* 2016 Apr-Jun;22(2):1182-1185. DOI: http://dx.doi.org/10.5272/jimab.2016222.1182

Received: 22/04/2016; Published online: 29/06/2016

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