Dr Artur Romaszewski
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
artur.romaszewski@uj.edu.pl

Dr Wojciech Trąbka
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
krzysztof.gajda@uj.edu.pl

ELECTRONIC MEDICAL RECORDS – HEALTH DATA PROCESSING OUTSIDE PLACE OF HEALTH CARE SERVICE PROVISION

Introduction

2018 is the subsequent deadline for the introduction of the electronic form of storing medical records (EMR) in the Polish health care system. Irrespectively of the delay, electronic processing of medical data has been implemented in an increasing number of health care entities. The paper form of records is being gradually replaced by an electronic form and this applies to the majority of entities that provide health care services and store medical records

despite the fact that the regulations introducing EMR as a standard have been changed several times.

There has recently been a trend to turn from the idea of a complex electronic document to the concept of a mandatory use of three standardized documents: a hospital discharge summary, hospital admission refusal note and a written information of a specialist to a referring physician[1]. There are also such separate electronic documents as e-prescription, certificate of temporary incapacity to work due to illness, hospitalization certificate or a certificate on in-patient treatment in any health care entity, a certificate on the responsibility of the provision of care for a family member (the so called L4 form). Electronic services are mainly registered in databases. Consequently, a problem arises how the data should be processed, i.e . how it should be maintained, stored and adequately secured.

The implementation of EMR as a mandatory form results in the responsibility of service providers to make crucial decisions as regards the introduction of computer systems to process electronic medical data. One of the decisions concerns entrusting the data to entities that deal professionally with data processing.

Oursourcing as a possible solution

Generally, the managers of entities that provide health care services have two options:

1. to process the data on premises (of a health care entity), which results in their consent for procedures that comply with legal regulations,
2. to transfer the data under adequate agreements to entities that professionally process data in other locations and to delegate to them all responsibilities as regards data security.

Both solutions have various options as regards technical and legal and administrative issues. When considering the uniqueness of medical data and their legal determinants as well as the specific features of health care entities, at a first glance the on-premises processing may

[1] Information concerning legal regulations as regards EMR 05.05.2017 https://www.csioz.gov.pl/aktualnosci/szczegoly/komunikat-dotyczacy-regulacji-prawnych-w-zakresie-elektronicznej-dokumentacji-medycznej/

seem a good solution as the health service provider fully controls the hardware, software and data processing. It also results in a complete responsibility for the credibility, integrity, security and confidentiality of medical data.

However, due to the uniqueness of medical (personal and sensitive) data and the legal and organizational requirements concerning medical data processing systems, the development and maintenance of a local computer center is a huge logistical and financial challenge. Suitable premises, the development of the network, the purchase of adequate hardware and software, as well as the employment of a highly qualified IT personnel generate substantial costs. Thus, such a solution seems to be realistic in major health care entities. However, the majority of health care service providers such as Primary Care Clinics, specialist, nursing or rehabilitation health centers will be unable to meet the above listed requirements. Moreover, the concept of an integrated health care information system, the cooperation with the Medical Information System (SIM) and with the platforms that service the health care system impose additional requirements on the existing systems.

As a result, the best solution for the majority of health care service providers seems to be outsourcing that is offered in various forms or cloud computing, which is currently a rapidly developing concept.

The outsourcing of services –such as the colocation and hosting services and particularly cloud computing for data processing as well as the storage of data and the software – ceased to be a novelty and became a standard way of keeping records. Thus, one should be able to answer the following question: What is the recent state of affairs as regards entrusting medical data with regard to the law and current standards and norms that have been developed for the purpose of secure processing in cloud computing?

The Authors make an attempt to analyze the problem from a practical point of view in order to help the managers of health care service entities make decisions as regards locations where medical data should be processed. Moreover, in the cases where the decision has been made, some essential pieces of advice will be made that concern signing or changing agreements with the providers of such services.

New legal regulations regarding medical data processing

The decision about the processing method of data in medical records is often influenced by the information about the security of health data that are stored in an electronic form. That

does not only concern all the systems that are used to process data located in hospitals, clinics, doctor's offices and organizations that group health care entities but also the systems that process the data entrusted by medical service providers. However, according to the reports, the data – mainly the data that are processed in hospitals – are not protected sufficiently. This is an acute problem as according to Europol forecasts the sensitive medical data of patients that are stored in insufficiently secured hospital systems are going to be the main object of attacks in 2017.

In 2015 in the US there were approximately 111 million cyberattacks in the health care sector which affected 35% of American people. In the most significant incident of this type – the attack on the Anthem company – there was a leakage of data of over 78 million patients. It is estimated that in 2017-2021 the total value of the global cybercrime damages will amount to $6 trillion and the necessary spending in cybersecurity will amount ot at least $1 trillion[2].

The most important legal regulations concerning the above issues are:

- the act of 6 November 2008 on patients' rights and the Commissioner for Patients' Rights[3],
- the act of 28 April 2011 healthcare information system[4],
- the act on personal data protection[5].

Due to the fact that new EU regulations will enter into force (May 2018), the adequate future GDPR provisions should be currently considered. With regard to personal data protection – including health data – an important source of information in the field of data security is constituted by the guidelines of the so called Article 29 Working Party[6], an independent European advisory body on data protection and privacy.

---

[2] Krakowiak J., *Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia*, http://www.rp.pl/Zadania/302079937-Dane-osobowe-Cyberbezpieczenstwo-a-sektor-ochrony-zdrowia.html#ap+1

[3] Journal of Laws 2009 No. 52 item 417

[4] Journal of Laws 2011 No. 113 item 657; Art. 9a. 1.

[5] Act of 29 August 1997 on personal data protection; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - GDPR (General Data Protection Regulation)

[6] Appointed by Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf

When discussing the data security issue one should also mention the regulations of the NIS Directive, i.e. the Directive of the European Parliament and European Commission concerning the measures to ensure a high common level of network and information security across the Union. The regulation will concern the choice of essential services operators (health care including) and digital service providers (online marketplaces, search engines and cloud computing). In other words providers of services for the health care sector, including cloud computing operators, will be recommended by the state[7].

Another significant problem as regards cloud computing is the long time dispute between EU and US about the security of the personal data of citizens of countries from the European Economic Area. This is because of the fact that cloud resources are often located outside Europe and belong to entities that apply other legal regulations (e.g. US). Since 12 July 2016 new rules of data transfer from EU to US have been in force – the so called privacy shield[8].

One should point out to the fact that with regard to this issue strong European bodies are formed. Thanks to that, conditions are created for a problem-free personal data processing in EU and, moreover, the tools developed by GDPR can be implemented to ensure the security standards of data processing – health data including. It should be emphasized that Cloud Infrastructure Services Providers in Europe, CISPE – a newly formed coalition of over 20 cloud service providers operating in Europe – announced the introduction of a first Data Protection Code of Conduct. Pursuant to this document, the cloud infrastructure service providers are obliged to offer their clients the opportunities to process and store data only within the territories of EU and EEA[9].

Data processing contract

Signing a contract for data processing is the final - and the only acceptable - form of entrusting data to an external entity. However, before that, several operations have to be made

---

[7] *Grzybowski M., Dziewięć faktów o Dyrektywie NIS, które powinieneś znać. http://itwadministracji.pl/numery/pazdziernik-2016/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac.html*

[8] European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, Brussels; European Commission decision No. C(2016) 4176 of 12 July 2016 r. http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[9] https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58e6909f16b49.pdf

as regards the collection of information about the service provider and the technology it applies. It is obvious that the manager of a health care entity who decides on the implementation of cloud computing in the processing of patients' data is not capable of assessing the technological capacities, functionality and the security level of a particular cloud computing service without some professional assistance. However, with some professional support adequate documents or service provider's information can be obtained about the technological solutions and the required security standards applied. If possible, one should get acquainted with the technical documentation of the solutions which should also be assessed by people or entities sufficiently qualified to do it. [10].

It is advisable that certified entities are given the opportunity to conduct an audit of a cloud computing provider. Such entities should present information about the members of the auditing team, their experience, qualifications and security certificates[11]. The contract should include provisions ensuring the security of data that the auditors have access to; it should also define the terms and the duration of the audit[12.] The negotiations with service providers are not always possible. Cloud computing agreements are frequently nonnegotiable; they are signed by a simple acceptance of the regulations and they often do not protect the client sufficiently. Typical market processes such as takeovers, bankruptcies or the liquidation of entities that provide cloud computing services to health care entities also pose a significant problem[13].

Data processing contract – legal regulations

[10] For example by the certificate of compliance with 27001/27002:2013, which is a commonly applied international standard of information security management, ISO/IEC 27018 as regards PII data protection or the *Cloud SecurityAlliance Cloud ControlsMatrix* [CCM] which describes the core protection principles that should be applied by service providers

[11] It is recommended that the security auditor should have the CISA (*Certified Information Systems Auditor)* certification while the remaining team members certifications confirming their IT security competencies, e.g. : CISSP (*Certified Information Systems Security Professional*); CISM (*Certified Information Security Manager*), or equivalent ones. The audit should be preceded by signing a contract with the auditing entity.

[12] Recommendations of Centrum Systemów Informacyjnych Ochrony Zdrowia (Centre for Health Care Information Systems) on safeguards and technological solutions applied in EMD processing; Appendix No.5 https://csioz.gov.pl/fileadmin/user_upload/zalacznik_nr_5_58e690a2325ef.pdf

[13] Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo; Source: gazetaprawna.pl Article of 18.10.2015, Author: T. Jurczak http://www.giodo.gov.pl/plik/id_p/9866/j/pl/

The legislator reacted to such state of affairs. The possibility to use the services of external entities to process health data has been regulated. The records can be entrusted to entities that specialize in providing services related to the management of sensitive health data.

First of all, the issue was resolved of the possibility of health service providers to take advantage of the data processing services offered by external entities. On the whole, the use of such services is acceptable. For the provision of external services (cloud computing included) to be legal, an agreement has to be signed as regulated in the act of 29 August 1997 on personal data protection.[14] Some publications[15] point at the fact that the lack of the possibility to indicate a data processing area in legal security documents[16] constitutes a legal obstacle. Even if the problem is valid, it is going to be solved after GDPR enters into force.

The entrustment of data processing occurs both in the cases when the data are transferred from a health care entity to external entities for processing on a permanent basis (e.g. the use of the software to develop medical documentation) and in ad hoc situations when the hardware with patients' data has to be serviced or when personal data of employees are transferred to medical entities offering occupational health services

A transfer of data by a health care entity in cases provided by law is not an entrustment of data. The same applies to the transfers of data by entities that keep health data registers, also the ones in the cloud. The transfer of data to registers is conducted under legal obligation. [17]

The agreement in question should meet the following conditions: [18]

- it is concluded in writing; solely within the scope and for the purpose as determined in the agreement to provide security measures protecting personal data and to ensure the supervision by the health care service provider that data processing is conducted in compliance with the agreement,

[14] Art. 31 par. 1
[15] Recommendations of Centrum Systemów Informacyjnych Ochrony Zdrowia (Centre for Health Care Information Systems) on safeguards and technological solutions applied in EMD processing
[16] Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on personal data processing documentation and technical and organizational conditions which should be fulfilled by devices and computer systems used for processing personal data ; Journal of Laws 2004 No. 100 item 1024
[17] Art. 4. Act of 28 April 2011 on health care information system, Journal of Laws 2011 No. 113 item 657

[18] Art. 31. Act of 29 August 1997 on personal data protection, Journal of LAws 1997 No.133 item 883

- health care services are not disturbed, particularly as regards the accessibility to data in medical documentation without undue delay,

- the processor is obliged to keep confidential the information about the patient (also after the death) which was obtained with regard to the agreement.

In the cases when the processing entity ceases to process personal data included in medical records, and particularly in the cases of its liquidation, it is obliged to transfer them to the entity that entrusted the data.

Health data in registers

The Minister of Health decides on establishing, keeping or contracting to keep medical registers by an entity. A register is an ordered set of data and information about illnesses and diseases, health condition, methods of treatment, diagnosing and monitoring of the progress in treatment as well as disease-related hazards. The significance of registers has been increasing with the implementation of electronic forms of communication.

The data are transferred to registers by

- service providers,

- entities that keep public and medical registries.

Within the period of 30 days after the commencement of personal data processing, the subject that runs a register should inform every data subject in the register about:

- its address and full name,

- the purpose, scope and method of data processing,

- the right to access to his/her data and to correct them,

- the category of recipients of the registered data,

- the optionality or obligation to provide the data that are processed in the register and, in the case of the latter, the legal basis.

In order to ensure the security of data in the course of the ITC system operations, the **data controller can authorize** an entity that keeps a medical register to **entrust** the processing of data included in the register to subjects that specialize in maintaining technical and system infrastructure providing technical services of ITC systems.

These subjects are obliged to provide organizational and technical measures that would ensure the protection of data processing, particularly the protection against unauthorized access, disclosure or takeover, modification, damage, destruction or loss of the data. The data in medical registers cannot be transferred for processing to other subjects. The specialized subjects are obliged to keep confidential the information about service recipients that was transferred for processing. The condition of confidentiality is in force also after the service recipient's death. In the course of processing **high level**[19] of security should be applied. The controller can supervise the subjects that specialize in providing technical service of ITC systems with respect to the observance of the requirements and methods of the accomplishment of the purposes of the entrustment of data that are processed in medical registers.

Entities that specialize in providing technical support to ITC systems and the subjects that keep medical registers are obliged to transfer the data to the controller (i.e. the Minister of Health) in the cases when the processing operations are stopped (particularly in the cases of liquidation). The Minister of Health may authorize an entity that keeps a medical register to take over the data.

The fact that is important and is subject to change when GDPR come into force is the issue of the liability for the data. At present, it is the data entrusting entity that is made liable. In the case of health care sector it is usually the subject that runs a health care entity. The subject that is entrusted the processing (the processor) does not become a data controller. Both subjects: the entrusting one and the one that is entrusted the processing are data controllers. A separate liability is introduced for the processor and the controller. Moreover, the processor is going to have the same responsibilities (at present the processor has to secure the data)

The controller should use the services only of the processors who guarantee the implementation of adequate technical and organizational measures that meet the requirements of GDPR and protect data subjects. Thus, the controller is imposed the obligation of due diligence as regards the selection of the processor. It seems that the assessment whether the

[19] as in provisions issued under the act of 29 August 1997 on personal data protection, Art. 39a

processor meets the requirements of the above GDPR provisions could be conducted after the controller's inspections of the data protection measures applied. However, there were no precise provisions in the act of 29 August 1997 on personal data protection with respect to this issue. As a result, the processors frequently block the possibilities of inspections. With a vast number of processors in Poland, a relatively insignificant number of them implemented data security protection on a level that would not result in their reluctance to an inspection that could possibly lead to breaking up further cooperation.[20] GDPR imposes the obligation to provide the controller or an authorized auditor the opportunity to conduct such audit.

Moreover, the following necessary elements have been indicated that the controller will have to provide in the agreement:

- the subject-matter and duration of the processing,
- the nature and purposes of the processing,
- the type of personal data and categories of data subjects,
- the responsibilities and rights of the controller

The following requirements as regards the processor are introduced:

- personal data processing can be conducted only under a written authorization of the controller,
- the processor ensures that persons authorized to process personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality,
- technical and organizational measures are implemented to ensure a security level adequate to the risk to the rights or freedoms of natural persons (the measures may include pseudonymisation and encryption of personal data, the assurance of confidentiality, integrity, availability and resilience of processing systems and processes, restoring the availability and access to personal data in the event of

[20] Bargiel-Kaflik M., *Kilka słów o tym, jak na gruncie GDPR powierzyć dane do przetwarzania* http://gdpr.pl/slow-o-tym-gruncie-gdpr-powierzyc-dane-przetwarzania/

physical or technical incident, regular testing and assessing the effectiveness of the above mentioned measures),

- the processor assists the controller for the fulfilment the controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR [21];

Bibliography:

[1.] Bargiel-Kaflik M., *Kilka słów o tym, jak na gruncie GDPR powierzyć dane do przetwarzania* http://gdpr.pl/slow-o-tym-gruncie-gdpr-powierzyc-dane-przetwarzania/

[2.] Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo; Source: gazetaprawna.pl: 2015-10-18; Author: T. Jurczak http://www.giodo.gov.pl/plik/id_p/9866/j/pl/

[3.] Journal of Laws 2009, No. 52 item 417

[4.] Journal of Laws 2011, No. 113 item 657; Art. 9a. 1.

[5.] Grzybowski M., *Dziewięć faktów o Dyrektywie NIS, które powinieneś znać.* http://itwadministracji.pl/numery/pazdziernik-2016/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac.html

[6.] https://www.csioz.gov.pl/aktualnosci/szczegoly/komunikat-dotyczacy-regulacji-prawnych-w-zakresie-elektronicznej-dokumentacji-medycznej/

[7.] https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58e6909f16b49.pdf

[8.] European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, Brussels; European Commission decision No. C(2016) 4176 of 12 July 2016 r. http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[9.] Krakowiak J., *Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia*, http://www.rp.pl/Zadania/302079937-Dane-osobowe-Cyberbezpieczenstwo-a-sektor-ochrony-zdrowia.html#ap-1

[10.] Recommendations of Centrum Systemów Informacyjnych Ochrony Zdrowia (Centre for Health Care Information Systems) on safeguards and technological solutions applied in EMD processing; Appendix No.5 https://csioz.gov.pl/fileadmin/user_upload/zalacznik_nr_5_58e690a2325ef.pdf

[11.] Act of 28 April 2011 on health care information system, Journal of Laws 2011 No. 113 item 657

[21] GDPR Art. 28 par. 3

[12.] Act of 29 August 1997 on personal data protection, Journal of Laws 1997 No. 133 item 883

[13.] Act of 29 August 1997 on personal data protection; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Abstract

The introduction of EMD as a mandatory form of keeping medical records results in the necessity for health service providers to make key decisions as regards the processing systems of digitized medical data. The managers of health care entities have two options: either to process the data on premises (of a health care entity), which results in their consent to proceed in compliance with legal regulations or to transfer the data under adequate agreements to entities that professionally process data in other location than the health care entity and consequently to delegate to them all responsibilities as regards the security of data.

Cloud computing – a rapidly developing solution – may be one of the options. The use of external entities to process health data has been regulated. Medical data can be entrusted to entities that professionally process them. Signing a contract for data processing is the final - and the only acceptable - form of entrusting data to an external entity

It is crucial that a proper choice of a cloud services provider is made and a precise agreement is signed that includes security measures for the protection of health data that comply with local and European regulations.