ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

Dr Artur Romaszewski
Dr Mariusz Duplaga
Szczepan Jakubowski, MA
Department of Health Promotion, Institute of Public Health, Faculty of Health Sciences, Jagiellonian University Medical College
artur.romaszewski@uj.edu.pl

HEALTH DATA IN NEW LEGAL SOLUTIONS AND STRATEGIC DOCUMENTS OF POLAND AND EU

Introduction

The pandemic is not only a medical challenge but it also involves issues related to data processing in health care systems. The burdens that societies bear due to the pandemic result in the relegation of initiatives and regulations concerning more general issues. A good example on the national level is the regulation on medical records[1]. One should not forget that at least some of the regulations that are caused by the pandemic and originally introduce only temporary changes in data processing may ultimately be of long-term nature. The introduction of the e-delivery service to the legal system is an important solution. It is the consequence of the implementation of trust services in Poland pursuant to eIDAS (*Electronic Identification and Trust Services Regulation*)[2]. It seems that this new solution will be applicable in transferring electronic medical documentation. The regulation will result in an effective protection of electronic documents, including medical documents, against the risk of loss or any unauthorized alteration. As a result, the transfer of documents will be secure and the sender and recipient clearly indicated[3]. Cybersecurity activities[4] should also be taken into consideration. This is an issue that will soon be of great significance particularly in the areas of data transfer and data processing in cloud computing[5,6].

[1] Regulation of the Minister of Health of April 6, 2020 on the types, scope and templates of medical documentation and the method of its processing (Journal of Laws, 2020, item 666).
[2] Act of November 18, 2020 on electronic delivery (Journal of Laws 2020, item 2320).
[3] Act of November 18, 2020 on electronic delivery (Journal of Laws 2020, item 2320).
[4] Draft recommendation of the Minister of Digitization on technical and organizational conditions for entrusting data to public administration for processing in a public computing cloud (Project 2018.07.09).
[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENSA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EFA relevance), p. 881.
[6] .Cloud computing is a model in which, in real time, the user leases computer resources such as storage, computer power and other network resources while having minimal interaction with the provider.

1. Single European Data Space

National regulations depend largely on the legislative activities of EU. The most significant regulations and documents include the Regulation on free flow of non-personal data[7], the Directive on open data[8], Commission Recommendation on a European electronic health record exchange format[9] and the European strategy on data[10].

The objective of the Strategy on data is to build a single European data space - a common, open market for data that is based on clear principles which include:

- free flow of data within and out of EU as well as across sectors;
- respect to European rights, principles and values, in particular personal data protection, consumer protection legislation and competition law;
- fair access to data and clear data governance mechanisms.

The strategy refers to personalized medicine as an area particularly important to societies in terms of the application of large data sets. The document states that "Personalized medicine will better respond to the patients" needs by enabling doctors to take data-enabled decisions. This will make it possible to tailor the right therapeutic strategy to the needs of the right person at the right time, and/or to determine the predisposition to disease and/or to deliver timely and targeted prevention"[11].

"The European strategy for data" defines four most significant pillars that are the basis for data processing[12]:

Pillar I – Data governance. This includes the issues of the data storage standards, clear principles on who can use the data and whose data can be used and how individuals can share the data that is generated by them.

Pillar II – The development of a data-based economy. The solutions that are implemented within this pillar aim at the development the European data space and a common cloud infrastructure.

[7] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2016 on a framework for the free flow of non-personal data in the European Union (Text with EFA relevance).
[8]. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
[9] Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format (text with EFA relevance).
[10] Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data. COM/2020/66 final, p. 66.
[11] European Commission website, „European Data Strategy".
[12] European Commission website.

Pillar III – Empowerment of citizens; the competencies of and the support for SMEs. The objective of this area of activities is to increase the individuals' rights to make decisions on their personal data and to ensure their control over non-personal data, e.g. the data generated by the Internet of Things (IoT), including health monitoring devices.

Pillar IV – Common European data spaces. The main purpose of this pillar is to develop a European infrastructure for data in the strategic sectors of economy, including a *Common European health data space*. Tools and architectures are planned to be developed that would facilitate the storage and use of data as well as sharing it among sectors.

The assumption is that the space will be designed in full compliance with the European data protection rules and the highest standards of ICT security.

Soon, health-sector specific legislative measures and other solutions will be developed that are necessary for the creation and functioning of the European health data space. The objective is to strengthen the access of citizens to their health data, to guarantee the transfer of the data and to eliminate barriers in cross-border provision of digital health services and products. An important assumption of the strategy is to increase empowerment of citizens in terms of their personal data. Thus, personal data spaces will be developed where citizens will be in control of their data and have the right to grant permission for its use[13].

Regarding the development of the European health data space there are plans to deploy data infrastructures and to provide tools and computing capacity that are adequate to the requirements of the project. This concerns mainly the support of the national electronic health records and the interoperability of health data through the application of the electronic health record exchange format. Cross-border exchange of health data will be developed through linking and using secure federated repositories, specific kinds of health information such as electronic health records, genomic information and digital medical images.

In compliance with the strategy, electronic documents will be provided. This includes electronic patient summaries and ePrescriptions between 22 member states participating in the eHealth Digital Service Infrastructure, eHDSI[14,15] and the initiation of cross-border eHDSI-based exchanges of medical images, laboratory results and discharge reports. There are plans

[13] Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data. COM/2020/66 final, p. 66.
[14] These two types of digital services will gradually be implemented until 2021 in the following 22 EU states: Austria, Belgium, Croatia, Cyprus, the Czech republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Luxemburg, Malta, the Netherlands, Germany, Poland, Portugal, Slovenia, Spain and Sweden.
[15] European Commission website, „Electronic Cross-Border Health Services".

to enhance the virtual consultation model and registries of the European reference network. Projects in the area of big data sets will be promoted and supported in order to support prevention, diagnostics and treatment (in particular for cancer, rare diseases and common and complex diseases), research and innovation, policy-making and regulatory activities in the public health area[16].

2. New form of Electronic Health Records (EHRs)

The development of IT technologies ultimately leads to a complete abandonment of developing and keeping paper records and results in switching to documentation in electronic form. Electronic medical documentation as the basic form of medical records was introduced In Poland by the Regulation of the Minister of Health of April 6, 2020 on the types, scope and templates of medical documentation and the method of its processing[17].

The Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format[18] is an important document. It defines the basic functions of electronic medical documentation. The health record exchange format that is accepted and implemented by all countries will facilitate easy sharing of the data among EU member states. Moreover, it enables EU citizens to access and share securely their health records across borders in the Union[19]. Ultimately, the individuals in EU will have the right to choose to whom they will share their electronic health data and to what extent. Importantly, the member states are obliged to introduce appropriate measures to support the application of interoperable EHRs.

EHRs should comply with the principles defined in the annex to the Recommendation. A legal basis or a clear consent of the person whose data are processes is the fundamental principle in the processing of health data. All data subjects should be guaranteed all rights under the General Data Protection Regulation (GDPR)[20] including the right of access to their health data in EHRs; this also refers to a cross-border access.

[16] European Commission website, „European Data Strategy".
[17] Regulation of the Minister of Health of April 6, 2020 on the types, scope and templates of medical documentation and the method of its processing (Journal of Laws, 2020, item 666).
[18] Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format (text with EFA relevance).
[19] Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format (text with EFA relevance).
[20] 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).

What is more, EHRs should be comprehensive. Every health data processing case has to be registered and verified for control purposes using appropriate methods such as keeping logs, creating auditing trails for the purposes of keeping precise records of access to the documentation, its exchange or any other processing operations.

The health data that is entered into EHRs should be machine readable in the scope necessary for the intended reuse. The information should be structured and coded in the most useful way so that the data is interoperable, also on the international level. Moreover, EHR systems should ensure the confidentiality of personal health data and comply with all aspects of data protection from the development stage.

3. Health data security

It is necessary to implement appropriate technical and organizational measures to ensure the security of EHR systems. They should be protected against unauthorized or unlawful processing of health data and against accidental loss, destruction or damage. Adequate training of the EHR staff must ensure awareness of cyber security.

A trustworthy and reliable identification and authorization of all interested parties (healthcare entities, healthcare staff, patients) is a crucial issue. This is an element that ensures trust to the exchange of data between HER systems. EU member states should take steps to make sure that the following health information domains constitute a baseline for the European health record exchange format:

- Patient summaries;
- ePrescriptions/eDispensations;
- Laboratory reports;
- Medical images and reports;
- Hospital discharge reports.

It is worth mentioning that EU member states already started sharing some elements of EHRs and exchanging the data among selected countries. Already in January 2019, Finnish citizens could buy medicines in Estonia using electronic prescriptions, and Luxemburg doctors will soon have the access to the records of patients from the Czech Republic[21].

Health care is an area which involves a wide use of the Internet and cloud computing. It is estimated that in the near future cloud computing will be the basic place of health data

[21] Gazeta Prawna, „KE chce ułatwić dostęp do dokumentacji medycznej w całej UE".

processing. This is caused by the fact that computer clouds have practically unlimited space for data storage and processing. However, there are some limitations to the application of such solutions. It is not the technological requirements that are the biggest barrier but the fact that legal regulations vary in countries where cloud computing is applied, which results in a varied approach to the data processed by the cloud depending on the registration of an entity or the place where the data is processed. The approach to the privacy of data and the access mode depend on the country where the entity with the network infrastructure is registered or on the location of data processing. This is particularly visible in the relations between US and EU with regard to personal data processing after the judgement revoking the previously applied bilateral agreements based on the US-EU Privacy Shield. The purpose of the program was to ensure the protection of personal data processed by American entities that would be equivalent to the one in Europe. However, EU Tribunal of Justice declared the invalidation of the Privacy Shield justifying it by the fact that American regulations provided too easy access to the data for US services[22] which was the consequence of the American Clarifying Lawful Overseas Use of Data Act (often referred to as the Cloud Act).

The above regulation gives access for American law enforcement authorities to digital data that is processed by American companies regardless of the legislation of the countries where the data is located and the citizenship, including the place of residence, of data subjects. It also allows the conclusion of executive agreements between the USA and other countries. The agreements give these countries the right to access personal data that is processed by American entities (except for US citizens, where a court order will still be the basis for surveillance)[23].

The GAIA-X initiative, **the European Data and Cloud Association**[24] is an attempt to overcome the deadlock. Its main objective is to become independent of American and Chinese providers of cloud computing services. GAIA-X is a commercial project. It aims at the support of innovation and digital transformation of EU. The concept of the project is based on European values and data processing regulations. Ultimately, a platform will be developed combining cloud services of dozens of companies and enabling service users to transfer data freely and

[22] Case C-311/18: Judgement of the Court (Grand Chamber) of 16 July 2020 - Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems.
[23] P. Opitek, *Clarifying Lawful Overseas Use Data Act – nowy model pozyskiwania danych cyfrowych w sprawach karnych, BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI*, 2018, p. 6.
[24] GAIA-X was established as a legal entity at the end of January 2021. It now has legal personality as an international non-profit association governed by Belgian law (AISBL).

securely – federative services based on common standards that ensure transparency and interoperability.

The main objectives of the GAIA-X[25] project are:

- to develop the values of federative services based on common standards that ensure transparency and interoperability;
- to integrate network, interconnection and cloud service providers;
- to integrate high-performance computing systems, sector- specific and edge clouds;
- to develop search mechanisms and the mechanisms of review and compilation services from participating providers in order to create a user-friendly infrastructure architecture;
- to develop minimum technical requirements and services that are necessary to operate the federated GAIA-X ecosystem;
- to develop services in compliance with the S*ecure by Design*[26] principles;
- to ensure the highest security and privacy requirements through the *Privacy by Design* concept.

The tasks of the GAIA-X association include the development of framework conditions in the following areas: architecture, interfaces, data classification, processes among the participating parties, interoperability and communication[27]. This means that fairly soon all data in member states, health data including, will be processed in a cloud located in Europe in compliance with the European legal regulations.

It should be pointed out that some Asian countries are implementing regulations similar to GDPR. Japan[28], for example, amended its *Protection of Personal Information Act in 2005*[29].

The assurance of health data security is a key challenge both in Poland and other EU countries. Until the end of 2020 there were over 90 incidents in Poland involving data security. There are reports about dangerous vulnerabilities in medical devices of several manufacturers. These concerned, among others, heart regulating devices of one of American manufacturers that had loops in Radio-Frequency Identification (RFID) protocols. The data could be "eavesdropped" from a close distance. Vulnerabilities were also detected in electrosurgical

[25] „GAIA-X: A Federated Data Infrastructure for Europe".
[26] *Secure by design* –software that is designed to be secure from the foundation stage
[27] Kancelaria Prezesa Rady Ministrów, Federacja Chmur Obliczeniowych - podsumowanie spotkania - Cyfryzacja KPRM - Portal Gov.pl.
[28] On January 23, 2019, the decision of the European Commission came into force, stating that the level of personal data protection in Japan is adequate to the system in the countries that belong to the European Economic Area.
[29] E. Woollacott, *Changes to Japan's Data Privacy Law Echo Europe's GDPR.*

devices of the same manufacturer and in the anesthesia equipment of another producer. While a theft of money from an account or an encryption of vital data may cause problems, an uncontrolled change in the parameters of medical devices may lead to the loss of health or life of patients, who – apart from the medical staff – are the most numerous group of users of such equipment. Cybersecurity incidents may effectively prevent surgeries or pose a danger to patients' privacy. The European Union Agency for Cybersecurity, ENISA)[30] recommends how to prevent attacks and what to do when they occur.

The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July concerning measures for a high common level of security of network and information systems across the Union[31] defines the principles of data processing in cloud computing on the EU level. The provisions of the directive define:

- the obligations of all member states to adopt national strategies for the security of network and information systems;
- cooperation groups and response teams to deal with computer security incidents;
- security and incident reporting requirements for the operators of key services and digital service providers, as well as the obligations of member states to designate appropriate national authorities, single contact points and networks of response teams[32].

In order to implement the above directive in Poland, the Act on the national security system was passed on 5 July 2018[33]. The Polish health care system is fairly efficient in the implementation of digitization processes. For example, the British system is much more reluctant to transfer health data to external servers, while in Poland the transfer to the cloud of the personal data contained in medical records by health centers or hospitals is practically a common practice[34].

Conclusions

[30] NASK, *Cyberbezpieczeństwo w ochronie zdrowia – kluczowe dla zdrowia i życia pacjentów.*
[31] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July concerning measures for a high common level of security of network and information systems across the Union.
[32] Act of 5 July 2018 on the national security system (Journal of Laws 2018, item 1560).
[33] Act of 5 July 2018 on the national security system (Journal of Laws 2018, item 1560).
[34] M. Wach, M. Puto, *Dane medyczne w chmurze – przyszłość czy rzeczywistość*.

We are witnessing a reorganization of electronic data processing systems in various sectors. Data sets incite innovations and facilitate monitoring of numerous important areas, including population health. The modification of such complex systems is possible by introducing top-down legislative guidelines. The main change involves the standardization of data processing electronic systems so that various users can freely, without any barriers, transfer data (for example between countries) – which is the Single European Data Space concept. Nevertheless, when introducing the changes the cybersecurity should not be forgotten. Consequently, it is necessary to implement appropriate technical and organizational measures to ensure cybersecurity of the systems; the GAIA-X initiative is a good example here.

Further research is necessary to assess the effectiveness of the solutions that are introduced both on national and European levels.

Bibliography

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data. COM/2020/66 final (2020).
[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July concerning measures for a high common level of security of network and information systems across the Union (N.D.)
[3] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (N.D.)
[4] European Commission website. „Electronic Cross-Border Health Services". Public Health - European Commission, 17 January 2019. https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.
[5] „European Data Strategy". European Commission. Accessed: 5 March 2021. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
[6] GAIA-X: A Federated Data Infrastructure for Europe. Accessed 5 March 2021. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.
[7] Gazeta Prawna. *KE chce ułatwić dostęp do dokumentacji medycznej w całej UE*, 6 February 2019. https://serwisy.gazetaprawna.pl/zdrowie/artykuly/1396362,ke-chce-ulatwic-dostep-do-dokumentacji-medycznej-w-calej-ue.html.
[8] Kancelaria Prezesa Rady Ministrów. „Federacja Chmur Obliczeniowych - podsumowanie spotkania - Cyfryzacja KPRM - Portal Gov.pl". Cyfryzacja KPRM, 31 sierpień 2020. https://www.gov.pl/web/cyfryzacja/federacja-chmur-obliczeniowych---podsumowanie-spotkania.
[9] NASK. *Cyberbezpieczeństwo w ochronie zdrowia – kluczowe dla zdrowia i życia pacjentów*. NASK. Accessed: 5 March 2021. https://www.nask.pl/pl/aktualnosci/3988,Cyberbezpieczenstwo-w-ochronie-zdrowia-kluczowe-dla-zdrowia-i-zycia-pacjentow.html.

[10] Opitek P., *Clarifying Lawful Overseas Use Data Act – nowy model pozyskiwania danych cyfrowych w sprawach karnych*, *BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI*, 2018, p. 6.
[11] Draft recommendation of the Minister of Digitization on technical and organizational conditions for entrusting data to public administration for processing in a public computing cloud (Project 2018.07.09). (N.D.)
[12] Regulation of the Minister of Health of April 6, 2020 on the types, scope and templates of medical documentation and the method of its processing (Journal of Laws, 2020, item 666). (N.D)
[13] Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format (text with EFA relevance) (N.D.).
[14] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2016 on a framework for the free flow of non-personal data in the European Union (Text with EFA relevance) (N.D.)
[15] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENSA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EFA relevance), (N.D.).
[16] Case C-311/18: Judgement of the Court (Grand Chamber) of 16 July 2020. - Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems. (N.D.). http://curia.europa.eu/juris/liste.jsf?num=C-311/18.
[17] Act of 5 July 2018 on the national security system (Journal of Laws 2018, item 1560) (N.D.).
[18] Act of November 18, 2020 on electronic delivery (Journal of Laws 2020, item 2320) (N.D.)
[19] Wach M., Puto M. *Dane medyczne w chmurze – przyszłość czy rzeczywistość*. *Cloud Community Europe Polska* (blog), 4 June 2020. https://cloudeurope.pl/dane-medyczne-w-chmurze/.
[20] Woollacott E. *Changes to Japan's Data Privacy Law Echo Europe's GDPR.* The Daily Swig | Cybersecurity news and views, 10 October 2020. https://portswigger.net/daily-swig/changes-to-japans-data-privacy-law-echo-europes-gdpr.
[21] Recommendation (EU) 2019/243 of 6 February 2019 on the European health record exchange format (text with EFA relevance) (N.D.)

Abstract

Due to their specificity and significance, health data are regulated by numerous legal strategic documents. The implementation of the concept of a Single European Data Space provides countries with the opportunity to share data, to be transparent and to guarantee the users the right to have control over their own data. Health data in electronic medical records should be machine-readable to the extent necessary for the re-use of the data. In response to the cybersecurity solutions that are applied in other countries, EU initiated the GAIA-X project whose aim is to become independent from American and Chines cloud computing service

providers. The objective of the project is mainly to support innovation and digital transformation in EU.

Key words:
health data, medical records, data space, cybersecurity, single digital market