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

PART II – HEALTH DATA IN THE LIGHT OF NEW TECHNOLOGICAL, LEGAL AND ORGANIZATIONAL CHALLENGES – SELECTED ISSUES

Introduction

In the opinion of the authors of this article, the Polish healthcare system succeeded spectacularly in the area of electronic services; this regards the e-Prescription service and the implementation of the Internet Patient's Account (IKP). As a result of this process, paper medical records in healthcare entities are being promptly superseded by electronic records. Moreover, after several years of discussions and changes of deadlines, new legal regulations[1,2] introduced electronic records as the basic form of medical documentation. This was a necessary step of a ten-year process towards the final full launch of the healthcare information system[3]. Although one should be optimistic about this fact, there are still several issues that should be considered in new regulations. This is caused mainly by the need to adapt national standards to EU regulations. First of all, the problem concerns the best use of such trust services as electronic signature, electronic seal, validation, preservation and the service of registered delivery. The use of these tools in the circulation and processing of electronic health documents, including electronic medical records (EMRs) is necessary for proper functioning of the healthcare information system. This is also necessary in the cross-border circulation of medical documents. The healthcare information system is a structure whose main priorities are the identification of entities involved in the development and processing of documents and the assurance of their integrity.

[1] Regulation of the Minister of Health of 6 April 2020 on the types, scope and templates of medical documentation and the methods of its processing (Journal of Laws 2020, item 666).
[2] Regulation of the Minister of Health of 8 May 2018 on the types of electronic medical records (Journal of Laws 2018, item 941).
[3] Act of 28 April 2011 on the information system in health care (Journal of Laws 2011, No. 113, item 657).

The article will discuss the above issues with the consideration of the legal regulations that are in force in the healthcare sector. Moreover, the authors will assess the applications of the new regulations of general nature for the purposes of healthcare. The aim is to sort out what regulations are in force; what regulations can be used and to draw attention to their shortcomings and deficiencies.

1. Legal challenges

The main legal regulation that constitutes the legal basis for the assurance of the security of electronic transactions and identity validation processes in electronic services is the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)[4]. eIDAS regulations were introduced to Poland by the Act of 5 September 2016 on trust services and electronic identification – some elements can also be found in the Act on the computerization of entities performing public tasks[5], while the Act of 18 November 2020 on electronic delivery[6], which is general in nature, can be additionally used in healthcare.

The regulations that are dedicated to the healthcare system are includes mainly 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[7], and the whole group of provisional regulations regarding Covid-19. The National Register of Patients with Covid-19[8] and telephone medical advice[9] are new solutions as regards healthcare services.

The solutions from the above legal acts were applied in healthcare regulations, i.e. in the regulations of the act on healthcare information system (concerning, inter alia, electronic medical records) as well as in the regulations on electronic medical records.

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[5] Act of 5 September 2016 on trust services and electronic identification (Journal of Laws 2016, item 1579).
[6] Act of 18 November 2020 on electronic delivery (Journal of Laws 2020, item 2320).
[7] 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).
[8] Regulation of the Minister of Health of 12 August 2020 on the organizational standard of telephone medical advice in primary healthcare (journal of Laws 2020, item 1395).
[9] Regulation of the Minister of Health of 12 August 2020 on the organizational standard of telephone medical advice in primary healthcare (journal of Laws 2020, item 1395).

Considering everyday activities of healthcare entities, reliable functioning of medical records services and the assurance of medical documentation security are the most important tasks. This is the reason why a legal act that would regulate developing, running and archiving medical records was much anticipated. The entrance into force of the regulation put an end to a long-standing dispute over the date of introducing electronic medical records as the basic form of medical documentation in healthcare entities. The introduction of the new regulations completed the difficult provisional period when healthcare entities processed documentation both in its electronic and paper forms. The present regulation does not allow record-keeping both in electronic and digital form. The principle is that documentation should be kept electronically, while the paper form is acceptable in justified and legally based situations.

2. Organizational and technological challenges

The pandemic resulted in a new type of service: the telephone medical advice. The first regulation concerning the telephone medical advice was introduced by the provisions of the COVID-19 special act of 2 March 2020[10]. The objective of the service was not to diagnose and treat patients but to group them into the ones who should have a stationary appointment and the ones who can have an online visit. The telephone medical advice served patients that phoned the national infoline service provided by NFZ (the National Health Service) only for Covid-19 cases. Doctors kept records of telephone medical advice and were obliged to keep them for 30 days from the date of the consultation, whereas online visits were regulated[11] before the pandemic and like stationary appointments were registered in patient's medical records.

The increase in the volume of data that is transferred by ICT networks and , first of all, the introduction of the principle that patient's records and information should be kept in an electronic form resulted in the necessity to ensure the security of the data .

The regulation of the Minister of Health of 31 October 2019 (par. 1, 5, 6)[12] dealt with this issue in a very general way by pointing to selected requirements concerning the security measures for medical information and ICT systems where the data is kept.

[10] Act of March 2 on special solutions related to the prevention, counteracting and combating COVID-19, other infectious diseases and the crisis situations caused by them (Journal of Laws 2020, item 374).
[11] Regulation of the Minister of Health of October 31, 2019 amending the regulation on guaranteed benefits in the field of primary healthcare (Journal of Laws 2019, item 2120).
[12] Regulation of the Minister of Health of 6 April 2020 on the types, scope and the templates of medical documentation and the method of its processing (Journal of Laws 2020, item 666).

The report of the Supreme Audit Office (NIK) [13] warned against cyber threat. The inspection showed numerous shortcomings with regard to the safeguards and the access to sensitive data that is stored in electronic medical records. The deficiencies included:

- Inadequate permission to access to patient data – this concerned nurses who were given access in HIS (Hospital Information System) to patient data from hospital wards or outpatient hospitals where they were not employed;
- Lack of appropriate authorizations to process patient personal data;
- Authorizations to individuals who should not process personal data;
- Failure to withdraw from former employees the rights to IT systems;
- Inadequate user authorization process in the operating system – individual logins and passwords were not given to individual employees; as a result groups of individuals (the employees of a particular hospital ward) applied the same authentication data in operating systems;
- In several hospitals it was possible to log in without authentication (operating systems could be started without logins and passwords);
- Passwords were not adequately complex;
- Employees involved in personal data processing were granted OS administrator rights despite the fact that their responsibilities did not include tasks related to the administration of IT infrastructure.

Numerous reservations of NIK concerned technical and organizational safeguards of health data protection. A vast majority of hospitals failed to apply appropriate technical measures to protect electronic personal health data. Some elements having an impact on security were improperly planned or applied. Other deficiencies included:

- the storage of data backup copies on the same device;
- the transfer of patient personal data as well as their health data in serving requests – this information was unnecessary to solve faults and the use of automatically assigned anonymized patient ID number was possible;
- the lack of appropriate security measures to safeguard electronic medical records;
- the lack of antivirus software or of current virus signature database.

[13] Najwyższa Izba Kontroli, *Wdrożenie Przez Podmioty Lecznicze Regulacji Dotyczących Ochrony Danych Osobowych*, Warszawa, 14 November 2019.

Practically, the human factor is essential in the functioning of healthcare entities. This fact has been known for ages and it is still crucial in the security assurance of data that is stored in the databases of medical institutions. In other words, the main responsibility for the security of data in the documentation is on the side of the adequately trained staff. There are cases where no technical measures can prevent misconduct in this area. This includes sending medical records as annexes to e-mails, taking photos of documentation by smartphones which are present on the location of data processing, taking the documentation out of the place where service is provided, sending the records to private mobile devices, transferring patient data on insecure data carriers or giving passwords to coworkers.

Moreover, outdated applications are used to develop EMRs and clinical applications are applied that were not designed to function securely in the current network environment. Another reason is the heterogenous nature of network systems and applications as well as the use of network-enabled devices in the same network as the entity's critical infrastructure[14].

Because of the above threats and – first of all – due to the importance of health data for the privacy of data subjects, it is obvious why legal regulations include provisions that aim at the maximum protection of the data. This is visible in the regulations concerning personal data protection, EMRs and data processing in the healthcare information and NFZ systems; a significant number of the regulations refer to technology. Unfortunately, this involves some problems as technical and legal concepts are used that are unfamiliar to most receivers, for example the trusted profile (the personal/qualified/advanced), electronic signature, the electronic seal, encryption and pseudonymization. What is more, the regulations refer to various types of norms and standards that in fact are incomprehensible to the recipients, which results in their resistance to the solutions. It is frequently difficult to understand the idea of the solutions and even more difficult to use them in practice. The fact that healthcare entities do not receive institutional assistance makes the problem harder. In addition, the varied interpretation of patient's rights is disturbing; this can be observed in everyday practice in the application of solutions in the Internet Patient Account. For example, the authorization issued by a patient for medical records is not respected and a paper statement must be completed again in a healthcare entity.

[14] J. Makuch, M. Guziak, *Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, Volume 14, No. 2, pp. 86-102, https://doi.org/10.34862/rbm.2020.2.6. (accessed: 16.03.2021).

The analysis of the new regulations concerning medical records shows that there are indications for appropriate technological solutions to be applied. The records should be signed either with a qualified electronic, trusted or personal signature or through a free application available in the ZUS ICT system that confirms the origin and integrity of the data. The signatures listed in the provisions should be used in line with the principle that the type of signature for particular operations is assigned by the legislator. More freedom of solutions was left for internal documentation. In these cases, records can be signed through internal mechanisms of the ICT system, which means that the decision is made by the head of a healthcare entity.

When analyzing the issue of electronic healthcare records, one should point out that there are numerous other electronic documents which are used on everyday basis that are involved with current operations and concern, for example, HR, accounting or health-related actions. In the development of electronic documents one has to be aware of the fact that the electronic signature cannot be denied legal effect or admissibility as evidence in legal proceedings solely on the basis that it is in an electronic form or does not comply with the requirements for qualified electronic signatures (Art. 25, par.1)[15].

The types of signatures are assigned to some of the above documents (this refers mainly to company reports – including financial statements) but in some documents this is not the case). Thus, an ordinary signature can be used to declare the identity of the signee. The ordinary electronic signature is not regulated in detail and its use depends on the signee's decision. The ordinary electronic signature is every addition made by a signature service of the information about the signee where the signee could make the decision on signing the document. Moreover, its credibility depends on how the document was registered by the signature service.[16] The qualified electronic signature may by EU law be substituted by a handwritten signature without the necessity to introduce new provisions to national legislations.

The cross-border nature of the signature should also be mentioned here. The qualified electronic signature that is based on the qualified certificate issued in one member state is recognized in Poland. Legal regulations provide for the mandatory requirement of the qualified electronic signature for selected documents. Currently, the documents that are signed

[15] Act of 5 September 2016 on trust services and electronic identification (Journal of Laws 2016, item 1579).
[16] *Zwykły, zaawansowany czy kwalifikowany podpis elektroniczny? Sprawdź jakie są różnice! | OSnews.pl.* http://osnews.pl/zwykly-zaawansowany-czy-kwalifikowany-podpis-elektroniczny-sprawdz-jakie-sa-roznice/ (accessed: 16.03.2021).

electronically in Poland are: annual financial reports, employee records, financial documents and powers of attorney.

The regulation on medical records ignores the institution of electronic seal. Contrary to the electronic signature, which is affixed to a particular natural person, the electronic seal is assigned to a legal entity. Electronic sealing results in the confirmation of the authenticity and integrity of a document. The electronic seal in a document confirms reliably that it was developed by an entity that is affixed to the seal and that the document did not change its contents[17]. In other words, the electronic seal in an electronic document guarantees that the electronic document originates from a particular entity (e.g. healthcare entity) and it contains particular information that cannot be changed (the principle of integrity). If the content of an e-document is changed after it is sealed, the verification stage will result in the notice that the seal is defective. The verification of a seal, as in the case of a signature, is possible through a certificate issued by an authorized entity, while the validation service makes it possible to obtain the information about the entity that used a particular e-seal. In conclusion, the electronic seal basically operates as the electronic signature. However:[18]

- the seal is used by a legal entity, company, office or organization;
- the seal is not a signature of the organization, i.e. its function does not involve representation and it is not used to make statements on behalf of the organization;
- the seal confirms the authenticity of a document – the document with the seal is issued by a particular organization;
- the validity of the qualified e-seal (the one that is certified in compliance with eIDAS) is implied – as it is in the case of the qualified electronic signature – and once it is issued in one member state, it cannot be rejected by another one.

Thus, the e-seal can work effectively in the areas that[19]:

- require a high-level assurance of document integrity and authenticity;
- prefer automatic document issue;

[17] M. Kostro, M. Tabor, *Identyfikacja i Uwierzytelnienie w Usługach Elektronicznych*, Związek Banków Polskich, Warszawa 2020, https://www.zbp.pl/getmedia/860b8ebd-4a6a-4fc9-a944-ddb8e9918f2a/ZBP_przewodnik_2020_v6 (accessed: 16.03.2021).

[18] *Report: Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce. 2017*. Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf (accessed: 16.03.2021).

[19] *Raport: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (accessed: 16.03.2021).

- shift the responsibility for an issued document to the company that used the e-seal (there is no need to look for the individual responsible for the e-document).

Internal documentation is the area of the healthcare system where particular electronic signatures (i.e. the electronic qualified, personal, trusted signature or the one issued by ZUS) are not required. Despite the proposed change in the provisions, the new regulation left unchanged the provision that allowed signing internal documentation with the use of internal mechanisms of the ICT system. This concerns mainly the solutions provided by IT companies together with the software for keeping electronic records. It seems that in such a situation it is possible to use the attributes of the e-seal (that is based on a qualified certificate) for documents with the ordinary signature and with the electronic seal. the common seal does not take advantage of the presumption of integrity and authenticity of the origin of the data related to the seal. Only the qualified electronic seal has this presumption[20].

Such a solution can be adopted in healthcare entities with regard to, inter alia, the records made available to the police, courts and prosecutor's office.

In their current operations, healthcare entities can adopt the solution that was introduced in 2016 - the document form of acts in law. In this case it is enough to make a declaration of intent in the form of a document in a manner that recognizes the identity of the declaration-maker. The document is any information carrier that makes it possible to acquire its content. Thus, the basic difference between this form and a written form (or a digital one) is the lack of the necessity to use a handwritten (or qualified electronic) signature. A document form is preserved - the signature is multiplied mechanically (e.g. a photocopy or a scan) in the case of a text document while e-mails include the first and the second name of the sender or the data allowing to establish his/her identity. In some cases clicking on the "Accept" button on the website will suffice. All these forms aim at affixing the individual that can be identified with the information that is stored electronically. Thus, the use of an ordinary electronic signature or an advanced electronic signature will be a document form.

3. Electronic registered delivery – a friendly and secure form of mutual data recognition

[20] *Grupa robocza ds. rejestrów rozproszonych i blockchain - Cyfryzacja KPRM - Portal Gov.pl*, https://www.gov.pl/web/cyfryzacja/blockchain (accessed: 12.03.2020).

Pursuant to eIDAS, Art. 3 par. 3, electronic registered delivery service is a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and which protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations[21]. The service is provided by a third party and consequently it cannot be provided by an institution or any other entity acting for communication with its clients. The built-in mechanism of third party ensures an independent source of evidence and a legal effect of sending and receiving data that is transferred by the electronic registered delivery service. In practice, the service in question guarantees security and effective protection against the loss of integrity and confidentiality of data being processed.

At present, the electronic registered delivery service is provided in EU only in five member states, among which Italy is the leader. Thanks to the implementation of this service, these countries have modern means to guarantee mutual recognition of data, to secure effectively communication in the healthcare sector and they enjoy a significant advance in the digitization of public administration services in a broad sense. In addition, the example of Italy points to an invaluable potential of electronic delivery as a tool to support remote communication and administrative services in the most difficult moments of the pandemic[22].

The Polish Act of 18 November 2020 on electronic delivery (Journal of Laws 2020, item 2320), which is to come into force on July 1, 2021, aims at defining the principles of exchanging correspondence of public entities both with other public entities or with non-public entities, including natural persons (the area of regulation will concern, inter alia, the relations between a citizen and a public administration entity or between a court and the parties of legal proceedings, as well as between a court and the above mentioned entities). Thus, in mid-2021 in Poland, a public service of electronic delivery will be put into use, which will provide digital confirmation of sending and receiving correspondence. This solution will introduce the principle of priority of electronic correspondence over the paper-based correspondence. It will also simplify current requirements for using electronic correspondence such as the consent to

[21] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[22] *Raport: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (accessed:16.03.2021).

electronic delivery in a given case, the consent to electronic delivery in the correspondence with a given entity, the electronic submission of an application or the registration in the system[23].

The functional architecture of the service to be introduced will follow the model described in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (European Journal 2014, L 256/73). Additionally, the Act provides for the implementation of a public hybrid service dedicated to digitally excluded individuals, which will enable them to receive paper-based documents from public entities that send them in a digital form by default[24].

In practice, the Act on electronic delivery imposes a number of new obligations to public and non-public entities that are subject to its provisions. The most important of them is the obligation of service between correspondents with the use of the public service of registered electronic delivery. A standard mail service is allowed only as an exception and only when the service delivery digital by default is ineffective. Another obligation is the need to transfer the address to the so-called electronic address database thanks to which the correspondence will be delivered each time to the address for electronic deliveries that is entered into the base. This, in turn, will enable receiving and viewing the correspondence in one place (i.e. in one delivery box) and in a uniform manner, and importantly – it will not disturb the access to online services provided by public entities. The entities that are subject to entry to the National Court Register (KRS) will be obliged to appoint the so-called delivery box controller, i.e. a person authorized to manage the mailbox (the management consists mainly in sending and receiving correspondence and assigning rights to individuals to perform operations in the mailbox) . For natural persons, in this case for the entities registered in ECIDG (the Central Register and Information on Economic Activity), the above option is possible but not mandatory. A new ICT system will be developed for the electronic delivery service provision[25].

[23] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (accessed:16.03.2021).
[24] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (accessed: 16.03.2021).
[25] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (accessed: 16.03.2021).

Conclusions

There is still a lack of detailed regulations on electronically signed medical records as regards, inter alia, the issue of digital preservation of the seal. With such significant changes in technologies and techniques of keeping electronic medical records, the legislator should consider organizing institutional support for entities implementing new solutions, for example by organizing regional tenders to assist entities that implement new solutions or by providing cloud solutions that offer software for keeping medical records.

Bibliography

[1] *Grupa robocza ds. rejestrów rozproszonych i blockchain - Cyfryzacja KPRM - Portal Gov.pl*, https://www.gov.pl/web/cyfryzacja/blockchain (accessed: 12.03.2020).
[2] Kostro M., Tabor M., *Identyfikacja i Uwierzytelnienie w Usługach Elektronicznych*, Związek Banków Polskich, Warszawa 2020, https://www.zbp.pl/getmedia/860b8ebd-4a6a-4fc9-a944-ddb8e9918f2a/ZBP_przewodnik_2020_v6 (accessed: 16.03.2021).
[3] Makuch J., Guziak M., *Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, V.14, No. 2, pp. 86-102, https://doi.org/10.34862/rbm.2020.2.6. (accessed: 16.03.2021).
[4] Najwyższa Izba Kontroli, *Wdrożenie Przez Podmioty Lecznicze Regulacji Dotyczących Ochrony Danych Osobowych*, Warszawa, 14 November 2019.
[5] *Report: Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce. 2017*. Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf (accessed: 16.03.2021).
[6] *Report: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (accessed: 16.03.2021).
[7] Regulation of the Minister of Health of 6 April 2020 on the types, scope and the templates of medical documentation and the method of its processing (Journal of Laws 2020, item 666)
[8] Regulation of the Minister of Health of 8 May 2018 on the types of electronic medical records (Journal of Laws 2018, item 941).
[9] Regulation of the Minister of Health of 12 August 2020 on the organizational standard of telephone medical advice in primary healthcare (Journal of Laws 2020, item 1395).
[10] Regulation of the Minister of Health of October 13, 2019 amending the regulation on guaranteed benefits in the field of primary healthcare (Journal of Laws 2019, item 2120).

[11] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[12] Act of March 2 on special solutions related to the prevention, counteracting and combating COVID-19, other infectious diseases and the crisis situations caused by them (Journal of Laws 2020, item 374)
[13] Act of 5 September 2016 on trust services and electronic identification (Journal of Laws 2016, item 1579).
[14] Act of 18 November 2020 on electronic delivery (Journal of Laws 2020, item 2320).
[15] Act of 28 April 2011 on the information system in health care (Journal of Laws 2011, No. 113, item 657).
[16] Wikarjak M., *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" November 1, 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (accessed: 16.03.2021).
[17] *Zwykły, zaawansowany czy kwalifikowany podpis elektroniczny? Sprawdź jakie są różnice!* | *OSnews.pl.* http://osnews.pl/zwykly-zaawansowany-czy-kwalifikowany-podpis-elektroniczny-sprawdz-jakie-sa-roznice/ (accessed: 16.03.2021).

Abstract

The progress in the transformation of paper-based medical records into their electronic form that results from legal regulations and organizational changes is a challenge to healthcare entities. Controls show that medical institutions make numerous mistakes, which may lead to cyber threat. Moreover, new (for the health sector) technological solutions are being developed such as trust services or registered electronic delivery, which improve the operations of the healthcare information system but require adaptation both on the part of the legislator and the medical entities themselves.

Key words

Data security, electronic medical records, trust services, telephone medical advice, healthcare information system