

The scope of identification in Health Care

(Obszar identyfikacji w sektorze ochrony zdrowia)

Sz Jakubowski ^{1,A,D}, A Romaszewski ^{1,C,F}, Z Kopański ^{1,E}, J Strychar ^{2,B}, M Liniarski ^{2,B},
T Kilian ^{2,A,B}

Abstract – The authors of the paper have introduced into the scope of identification, including the authentication in the health care sector, and highlighted the importance of proper national and international regulations creating new opportunities. They drew the attention to the current need of identification of the patient and the natural person or legal entity, providing medical service. A classic case of confirmation of the identity of the patient in Poland is present during a medical visit. The verification of entitlement takes place with the presentation of the ID based on the eWUŚ electronic system (Electronic Verification of Eligibility of Beneficiaries). The eligibility of the medical practitioner or diagnostician, on the other hand, can be verified in the electronic register of staff members, operating based on proper legal regulations.

Key words - identification, health care sector.

Streszczenie – Autorzy dokonali wprowadzenia w obszar identyfikacji, w tym uwierzytelniania w sektorze ochrony zdrowia, podkreślili znaczenie krajowych oraz zagranicznych stosownych regulacji tworzących nowe możliwości. Zwrócili uwagę, że współcześnie istnieje konieczność identyfikacji zarówno pacjenta, jak i osoby fizycznej/prawnej, która świadczy usługi medyczne. Z podstawowym przykładem potwierdzenia tożsamości pacjenta w Polsce mamy do czynienia podczas wizyty lekarskiej, gdzie sprawdzenie uprawnień następuje po okazaniu dowodu osobistego na podstawie systemu Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców (eWUŚ). Z kolei uprawnienia lekarza bądź diagnosty mogą być sprawdzone dzięki elektronicznym rejstrum pracowników, działającym w oparciu o stosowne regulacje prawne.

Słowa kluczowe - identyfikacja, sektor ochrony zdrowia.

Author Affiliations:

1. Faculty of Health Sciences, Collegium Medicum, Jagiellonian University
2. Collegium Masoviense – College of Health Sciences, Żyrardów

Authors' contributions to the article:

- A. The idea and the planning of the study
- B. Gathering and listing data
- C. The data analysis and interpretation
- D. Writing the article
- E. Critical review of the article
- F. Final approval of the article

Correspondence to:

Prof. Zbigniew Kopański MD PhD, Collegium Masoviense - College of Health Sciences, Żyrardów, G. Narutowicza 35 Str., PL-96-300 Żyrardów, Poland, e-mail: zkopanski@o2.pl

Accepted for publication: November 28, 2018.

I. INTRODUCTION

The scope of identification, including authorization in the health care sector, expands each year and the country and international employer create new opportunities through proper regulations. Nowadays, one may face the need of identification of the patient, as well as the natural person or legal entity, which provides medical service. A classic case of confirmation of the identity of the patient in Poland is present during a medical visit. The verification of entitlement takes place with the presentation of the ID based on the eWUŚ electronic system. The eligibility of the medical practitioner or diagnostician, on the other hand, can be verified in the electronic register of staff members, operating based on proper legal regulations [1].

Health facilities more and more often save patient's data in an electronic form creating electronic medical documentation, which requires authorization in terms of who created

it and confirmation of identity (in case of having access to it). It is so because of organizational and legal matters. The development of digital technology mainly in these communicational branches (Information and Communication Technologies - ICT) enables a relatively easy and quick data processing of patient's health condition and access to data. Further computer-based analysis can support the healing process of the patient. However, switching from traditional paper-based documentation, without an electronic system and internet access, to an electronic one (gathered on servers or cloud computing) carry new risk involving the lack of suitable protection of data storage and can not guarantee safety of the computerized system, which serves sending and sharing data [2].

Every day in the health care sector, large amounts of patient and health data are produced and processed. This information is of sensitive nature, which is subject to special protection. Loss of this data or blocked access of medical staff to them may hinder the treatment process, which in particular cases may threaten the life and health of the patient. In addition, the captured data of those being treated may potentially be illegally used by companies (e.g. insurance companies) to achieve their own goals or as a tool for blackmail [2]. According to data on American hospitals and smaller medical institutions, every tenth entity reports attempts to break into medical records systems [3]. The reason is often a lack of awareness and an appropriate knowledge of employees in the health care sector and an inadequate, underfunded information infrastructure associated with the lack of procedures which guarantee data security in the facility [2].

On account of the scale and the impact on the population of a potential medical data leak, the health care area is referred to as the critical sector. With the aim of securing the legal relationships, standards and effective risk management strategies are created. Additionally, knowledge from good practices is applied from the other institutions for example banking identification systems [2].

Identification and authentication are two of the most important processes for the protection of personal and medical data. That is why there are national and international regulations that are designed to develop principles, legal relationships and standards for the functioning of electronic systems, including here also medical electronic systems.

II. ENTITIES IN HEALTH PROTECTION

In health care entities, who conduct medical activities, are primarily responsible for creating and securing patient data in the form of medical records.

According to the act on medical activity (Journal of Laws 2011, No. 112, item 654) (4), a healing activity, consists in providing health services both directly or through communication and telemedicine systems. Additionally, in the field of health services, health promotion and didactic and research activities, for example introducing new methods of treatment. Moreover, health benefits can be divided into stationary / 24- hour health services (hospital or non-hospital) and health services in the outpatient setting. Entities, which are distinguished due to the organizational form may provide these services. These are: entrepreneurs, the independent public health care centers, the budgetary units, the research institutes, the foundations or the associations, a legal entity and organizational units, which operate on the basis of regulations on the relationship between the state and religious associations, and the military units. Moreover, the entities carrying out therapeutic activities include physicians, nurses and midwives conducting both individual and group practices [4].

Due to the specificity of authentication and identification in health care, entities carrying out therapeutic activities can be divided into two basic types, namely daily, non-stationary treatment called open (outpatient clinics, clinics, medical practices, medical centres, etc.) and in-patient, in-patient and in-patient treatment defined as closed (hospitals, nursing homes, nursing homes and others). The subject matter, type of data collected and medical documentation created by both groups differ greatly from each other. Moreover, there is currently no common system for electronic medical records from "open" and "closed" treatment. Equally important in the health information system in the medical area are pharmacies, medical supply companies and institutions such as the National Health Fund (public payer) and the Health Insurance Institution/Agricultural Social Insurance Fund (public insurance companies) [5].

II. ELECTRONIC DOCUMENT

An electronic document containing personal and medical (sensitive) data about a patient should be subject to specific

protection as regards the reliability of the data contained therein and the possibility of making it available to the patient and other entities, after prior identification and authentication.

First of all, in order to define the notion of medical data, it is necessary to understand what data in the general sense are. Data according to the Act of 28 April 2011 on the information system in health care (Journal of Laws of 2011 No. 113 item 657) (6) are: "letters, words, numbers, texts, numbers, signs, symbols, images, combinations of letters, numbers, numbers, symbols and signs, collected in collections of a specified structure, available according to specified criteria, including personal data". (Article 2(4)) [6]. Specifying and focusing on one specific category, medical data according to the Recommendation of the Council of Europe is all information in the field of health of a particular person, including genetic data [7]. Moreover, in Polish law, medical data defined as individual medical data shall be understood as "personal data and other data of natural persons concerning rights to provided, being provided and planned health care services, health condition, as well as other data processed in connection with planned, provided and being provided health care services and health prevention and implementation of health programmes" (Article 2 point 7). The above terms can be applied to both the physical form of records (e.g. on paper), as well as electronic form. Patient data collected in entities conducting therapeutic activity usually take the form of medical records. In Poland, however, there are no complete and clear legal regulations concerning the definition of medical records. The legislator has indicated what the documentation should contain, who can process it and what are its types.

Additionally, as stated in Art. 24 point 2 of the Act on Patient's Rights and Patient's Ombudsman (Journal of Laws of 2009, No. 52, item 417) [8]: to process data contained in medical records [...] in order to protect health, provide and manage the provision of health services, maintain the IT system in which medical records are processed, and to ensure the safety of this system the following persons are entitled :

- 1) medical practitioners;
- 2) other persons performing activities supporting the provision of health services, as well as activities related to the maintenance of the IT system in which the medical documentation is processed and ensuring the security of this system, on the basis of an authorisation of the data controller".

In turn, the regulation of the Minister of Health (Journal of Laws 2015, item 2069) introduces the division of medical documentation into individual and collective, and each of them additionally into internal and external [9]. Individual internal documentation prepared for the needs of a healthcare provider may constitute e.g. a history of health and disease.

A patient is the recipient of individual external documentation that takes the form of a prescription, referral, information card from hospital treatment, etc. The collective internal documentation owned by the provider constitutes various types of books and censuses, e. g. Patient's Book, Waiting Book. The last type is the collective external documentation prepared for external institutions such as payers, statistical or inspection institutions, in the form of statistical and settlement reports [10]. However, the above considerations did not include the context of electronic form, as will be the case below.

The Polish definition of an electronic document explains that it is a "separate whole meaningful set of data ordered in a specific internal structure and stored on an IT data carrier" (Article 3(2) [11], where the computer storage medium is " a material or device for recording, storing and reading data in digital form" (Article 3(1)) (11). Unfortunately, this definition is inconsistent with the understanding of the European legislator who, in order to systematise an electronic document in the European Union (EU) countries, describes it as "any content stored in electronic form, such as text, visual, audio and audiovisual recordings"[12]. Additionally, in this definition there is no indication of the data carrier, thus giving the freedom of the technology used to transfer the data [12].

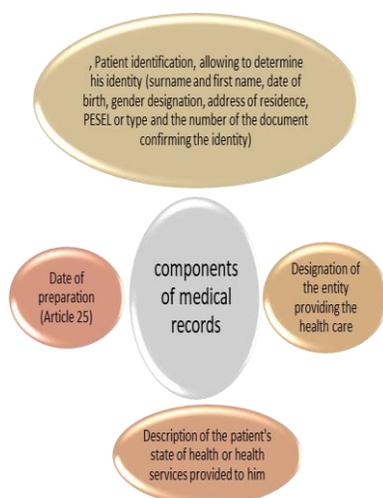


Figure 1. Components of medical records [8]

Knowing what features a medical and electronic document should contain, you can proceed to further deliberations and specify what an electronic document containing medical data, hereinafter referred to as an electronic medical documentation, is.

In Poland, it is indicated that electronic medical records are "documents created in an electronic form with a qualified electronic signature, a signature confirmed by a trusted profile of ePUAP (Electronic Platform for Public Administration Services) or with use of a method of confirming the origin and integrity of data available in the teleinformatic system that is made available free by the Social Insurance Institution (ZUS)" (Article 6) [13]. There appears a very important element of data security and a statement of their assurance thanks to techniques developed by ePUAP or the Social Insurance Institution (in Poland it is called "Zakład Ubezpieczeń Społecznych", in short – ZUS). There are currently three types of electronic medical records [14]:

- 1) "information about the diagnosis of a disease, health problem or injury, the results of the tests carried out, the reason for refusing admission to hospital, the health services provided and any recommendations – in case of refusal to admit a patient to hospital
- 2) information for the attending physician about the patient's diagnosis, treatment, prognosis, prescribed drugs, foodstuffs for particular nutritional uses and medical devices, including the period of their use, dosage regimen and appointed follow-up visits
- 3) patient information card from the hospital (§. 1).

The European Union legislator defines electronic medical documentation as: "comprehensive medical or similar documentation of the future and current physical and mental health of the person concerned, in electronic form, ensuring that the data are available for treatment or for other closely related purposes" [15]. Electronic medical documentation is subject to certain standards of creation so that it is possible to send documents between medical entities. One of the most important standards applied in Poland is the implemented international standard HL7 and the rules of its application are included in the document entitled Poland National Implementation HL7 CDA [16]. This study is intended mainly for IT service providers of medical entities and should help in the implementation of electronic medical records in accordance with generally accepted rules and standards. The mentioned document describes standards for two types of documents for medical units for their secure transmission. The first type is data that will be processed on

the P1 project platform (Electronic Platform for Gathering, Analyzing and Sharing digital content about Medical Events) and it will be e-Prescription, e-Referral and e-Order. The second type of documents, however, will not be processed on the P1 project platform, but only indexed on it. This group includes: "Medical consultation, hospital discharge summary, Laboratory test report, Description of the diagnostic test, Refusal of Admission into Emergency Room, Nursing care individual card (including: Nursing anamnesis card, Patient assessment sheet, Discharge card with directions for the patient, Nursing report), Entry to the immunization card and the Operational Protocol "[17].

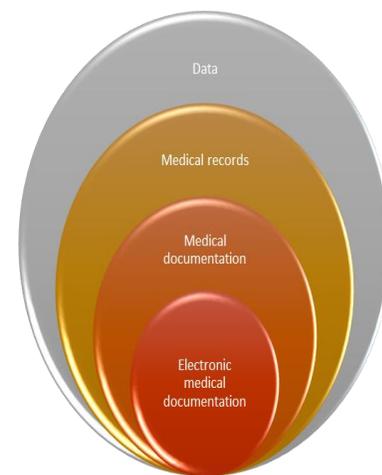


Figure 2. Data structure in health care [own elaboration]

III. ELECTRONIC IDENTIFICATION AND AUTHENTICATION

Identification is the "processes or result of the processes of identifying a given object (system, object) with another object (system, object) previously known" [18]. On the other hand, authentication is defined as "unambiguous identification of an entity authorized to use a given element of a computer system" [19].

On the other hand, identification, but more broadly in the electronic form, is understood as the process of using data in electronic form identifying a person that uniquely represents a natural or legal person or a natural person representing a legal person (Article 3).

The definition according to the Polish Committee for Standardization defines identification as "the process of automated recognition of a specific user in the system possible to implement thanks to the use of unique names" [1]. Data identifying a person is data that gives the possibility to assign a specific identity to a natural or legal person. The data package creates an identifier that can be included on a tangible or intangible tool called the electronic identification means [12].

Using this tool containing person identification data, it is possible to authenticate to online services (on the Internet). Authentication broadly means an electronic process that allows an electronic identification of a natural or legal person, or proof of the origin and integrity of verified data in an electronic form (Article 3) [12].

IV. REFERENCES

- [1] Romaszewski A, Trąbka W, Kielar M, Gajda K.: Identyfikacja i uwierzytelnienie w systemie informacyjnym opieki zdrowotnej po wprowadzeniu rozporządzenia UE eIDAS. Zesz Nauk Wyższej Szk Zarządzania Bank W Krakowie 2016;(41):1–23.
- [2] 2. Domański Zakrzewski P, Najbuk P, *i wsp.* Cyberbezpieczeństwo w sektorze ochrony zdrowia 2017. [online] [cited 2018 Mar 10] Available from: URL: www.dzp.pl
- [3] 3. KPMG. Health care and cyber security: Increasing Threats Require Increased Capabilities . [online] [cited 2018 Mar 10] Available from: URL: <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf>
- [4] 4. Ustawa z dnia 15 kwietnia 2011r. o działalności leczniczej.
- [5] 5. Kotuła J. Otwarta i zamknięta opieka zdrowotna w Zielonej Górze w latach 1945 – 1989. Stud Zachodnie 2016;18:237–70.
- [6] 6. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 nr 113 poz. 657) . [online] [cited 2018 Mar 10] Available from: URL: <http://prawo.sejm.gov.pl>
- [7] 7. Rekomendacje nr (97)5 Komitetu Ministrów Rady Europy z 13 lutego 1997. [online] [cited 2018 Mar 10] Available from: URL: <https://giodo.gov.pl/pl/230/1698>
- [8] 8. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009 nr 52 poz. 417) . [online] [cited 2018 Mar 18] Available from: URL: <http://prawo.sejm.gov.pl>
- [9] 9. Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069) . [online] [cited 2018 Mar 18] Available from: URL: <http://dziennikustaw.gov.pl>
- [10] 10. Nyczaj K, Piecuch P. Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej. Warszawa; Wiedza i Praktyka, 2014.
- [11] 11. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565) [Internet]. . [online] [cited 2018 Mar 18] Available from: URL: <http://prawo.sejm.gov.pl>
- [12] 12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE . [online] [cited 2018 Aug 28] Available from: URL: <https://eur-lex.europa.eu>
- [13] 13. Ustawa z dnia 1 marca 2018 r. o zmianie niektórych ustaw w związku z wprowadzeniem e-recepty (Dz.U. 2018 poz. 697) . [online] [cited 2018 Mar 18] Available from: URL: <http://prawo.sejm.gov.pl>
- [14] 14. Minister Zdrowia.: Projekt Rozporządzenia Ministra Zdrowia (2018 r.) w sprawie rodzajów elektronicznej dokumentacji medycznej. [online] [cited 2018 Mar 18] Available from: URL: <https://legislacja.rcl.gov.pl>
- [15] 15. Nyczaj K, Piecuch P. Dokument Roboczy Grupy Roboczej ds. Ochrony Danych Komisji Europejskiej za: Elektroniczna Dokumentacja Medyczna, Wdrożenie i prowadzenie w placówce medycznej. Wiedza i Praktyka; 2014.
- [16] 16. Pusz P. Centrum Systemów Informacyjnych Ochrony Zdrowia.: Instrukcja stosowania Polskiej Implementacji Krajowej HL7 CDA WERSJA 1.2 . [online] [cited 2018 Mar 18] Available from: URL: <https://www.csioz.gov.pl/HL7POL/pl-cda-html-pl-PL/>
- [17] 17. Centrum Systemów Informacyjnych Ochrony Zdrowia. Reguły tworzenia elektronicznej dokumentacji medycznej (wersja: 1.2) . [online] [cited 2018 Mar 18] Available from: URL: <https://www.csioz.gov.pl/HL7POL/pl-cda-html-pl-PL/>
- [18] 18. Internetowa encyklopedia PWN.: Identyfikacja . [online] [cited 2018 Mar 18] Available from: URL: <https://encyklopedia.pwn.pl/haslo/identyfikacja;4008495.html>
- [19] 19. Internetowa encyklopedia PWN.: Uwierzytelnianie . [online] [cited 2018 Mar 18] Available from: URL: <https://encyklopedia.pwn.pl/haslo/uwierzytelnianie;3992005.html>