Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 25–38
https://doi.org/10.31743/recl.18702
Received: 5 June 2025 | Accepted: 3 February 2026 | Published: 31 March 2026

Legal Regulation of Electronic Identity in eHealth Services in Poland and Estonia: A Comparative Analysis

Krzysztof Świtała

PhD, Department of Informatics Law, The Law and Administration Faculty, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Wóycickiego 1/3, 01–938 Warsaw, Poland; e-mail: k.switala@uksw.edu.pl
https://orcid.org/0000-0003-0426-5383

Abstract: The primary aim of the article is to analyze the role of electronic identity in ICT-enabled healthcare in the context of existing legal instruments in these areas, both at the EU level and in the regulations of selected Member States (Poland, Estonia). A basic analysis of eHealth, telemedicine, and EHR systems was conducted, considering the role of electronic identity in data processing within the health care information infrastructure. EU regulations such as eIDAS, the directive on patients' rights in cross-border healthcare, and the regulation on the European Health Data Space were taken into account. The role of electronic identity management systems in the context of the patient's right to medical services, consent, information about their condition, and the preservation of medical professional confidentiality and privacy is also discussed. Finally, existing electronic identification systems in Poland (*Profil Zaufany*, *Profil Osobisty*, *mObywatel*) and Estonia (e-ID), which are also used to authenticate patients accessing healthcare services in these countries, are presented.

Keywords: electronic identity, eHealth, eIDAS, healthcare, EHR

1. Introduction

Modern healthcare is increasingly dependent on information and communication technologies (ICT). The pace of change accelerated, particularly during the COVID-19 pandemic, when the burden of delivering outpatient health services shifted to a remote, decentralized format. Unfortunately, in Poland, these were not comprehensive and mature nationwide telemedicine solutions, but, in practice, only the exchange of voice messages between the patient and doctor via mobile phone services.[1] In the Scandinavian countries, a developed health care system, including modern electronic data processing technologies that incorporate eHealth services and support digitalization efforts, has enabled more effective coping with the challenges of maintaining efficiency and business continuity in this sector.[2] The implementation of ICT in healthcare should complement traditional forms of patient care, taking into account patients' welfare and respecting their rights.

[1] These are the conclusions from an analysis of results from the Ministry of Health and National Health Fund's survey of patient satisfaction with teleconsultations with their primary care physician during the COVID-19 epidemic ("Raport z badania satysfakcji pacjentów korzystających z teleporad u lekarza podstawowej opieki zdrowotnej w okresie epidemii COVID-19" [2020], accessed June 4, 2025, https://www.gov.pl/attachment/a702e12b-8b16-44f1-92b5-73aaef6c165c, 9).

[2] Suhail Muzaik and Nadia Davoody, "Exploring the Operational and Technical Changes in the Healthcare Sector During the COVID-19 Pandemic," in *Telehealth Ecosystems in Practice*, eds. Mauro Giacomini et al. (Amsterdam: IOS Press, 2023), 281.

ISSN 2545-384X (Online)

This article aims to present the legal role of mechanisms for managing and maintaining digital identity in contemporary ICT-enabled healthcare. The analysis will cover existing normative solutions at the EU level and in selected Member States, and will attempt to assess their consistency. To illustrate the issue of electronic identity institutions in the EU, legal solutions introduced by the eIDAS Regulation will be presented. As a use case, electronic identification methods for public and healthcare services in Estonia and Poland will be discussed.

Analysis of the normative material considered in this article was primarily carried out according to the comparative and dogmatic-legal methods, including the presentation and interpretation of legal provisions, a review of the literature on the subject, and the technical standards necessary to elucidate the context of the considerations.

2. eHealth, Telemedicine and EHR

In World Health Organization documents, eHealth is defined as the use of ICT in health care for purposes such as treating patients, conducting research, educating students, detecting disease, and monitoring the health of the population.[3] The scope of this term is not limited to technical and IT issues, but also encompasses other management tools, processes, and working methods that may have a positive impact on patient health and the quality of healthcare services in the information society. The technical standard ISO 27799 defines a concept related to eHealth – a health information system, understood as an electronically maintained health software (intended to be used specifically for managing, maintaining, or improving health of individual persons or the delivery of care – which also covers the adoption of medical devices) and repository of patient personal health information, collected and transmitted securely, and ensuring that these resources are only available to authorized users.[4] The role of identity management modules in ensuring the confidentiality of data processed in eHealth systems is outlined in the analyzed document.

Telemedicine is defined in EU documents as the provision of healthcare services through the use of ICT in situations where the health professional and patient (or group of health professionals) are not in the same location. It involves the secure transmission of medical data and information via text, sound, images, or other forms needed for preventive medicine, diagnosis, treatment, and patient follow-up.[5] Telemedicine solutions enable medical procedures to be performed at a distance (telesurgery), facilitate audio, visual, and text communication between medical specialists (teleconsultation), and enable the remote transmission and description of diagnostic tests (teleradiology) and the remote monitoring of patients (telemonitoring, including telecardiology, telecare).

---

3 "eHealth," World Health Organization. Eastern Mediterranean Region, accessed June 4, 2025, https://www.emro.who.int/health-topics/ehealth/.

4 *ISO 27799 – Health informatics – Information security controls in health based on ISO/IEC 27002* (Geneva: ISO, 2025), 2.

5 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*, COM(2008) 689 final (Brussels, November 4, 2008), 3.

Electronic Health Records constitute the basic collection of information about patients who receive medical services.[6] Pursuant to § 1(1) of the Ordinance of the Minister of Health of 6 April 2020 on the types, scope, and models of medical records and the manner of their processing,[7] there is an obligation in Poland as of 2019 to keep patient medical records exclusively in electronic form. In accordance with Article 3(m) of Directive 2011/24/EU,[8] medical records mean all the documents containing data, assessments, and information of any kind on a patient's health and clinical evolution throughout the care process. The content of Article 2, point 6 of the Act of 28 April 2011 on the healthcare information system[9] specifies that the EHR consists of documents created in electronic form with a qualified electronic signature, trusted signature, personal signature, or using the method of confirming the origin and integrity of the data available in the ICT system of the Social Insurance Institution (Polish: *Zakład Ubezpieczeń Społecznych*). It should be noted that the definition under consideration emphasizes the importance of using user authentication mechanisms to ensure that EHR processing complies with legal obligations.[10] In EU legislation, the discussed medical records concept is understood as a collection of personal or non-personal electronic health data related to a natural person, collected in the health system and processed for the purpose of providing healthcare (Article 2(2)(j) of Regulation 2025/327). Summarizing the definitions cited above, it can be concluded that the EHR is an appropriately secured set of electronic patient data, constituting a separate, meaningful content and organized in a specific internal structure, processed for the purpose of performing health care tasks. Analysis of the cited definitions leads to the conclusion that eHealth, in fact, encompasses both telemedicine services and EHRs within its scope. Proper functioning of these solutions is not possible without ensuring an adequate level of security covering confidentiality, integrity, authenticity, and accountability for the resources processed in these systems and, mostly, the realization of the rights of their users. This means that electronic identity management systems are a necessary and integral part of this information infrastructure.

3. Electronic Identity

Electronic identity (eID) is a basic component of the knowledge economy and information society.[11] According to ISO 24760–1 technical standard, identity is a set of attributes related to an entity – item relevant for the operation of a domain (environment) that has

6 Urszula Drozdowska et al., *Dokumentacja medyczna* (Warszawa: Eskulap, 2011), 21–22.

7 The Ordinance of the Minister of Health on the types, scope and models of medical records and the manner of their processing of 6 April 2020, Journal of Laws 2024, item 798.

8 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4 April 2011).

9 Act on the healthcare information system of 28 April 2011, Journal of Laws 2025, item 302.

10 Zuzanna Maj, "Elektroniczna dokumentacja medyczna – wybrane aspekty prawne," *Przegląd Prawa Medycznego* 4, no. 1 (2022): 121–22, https://doi.org/10.70537/14y42909.

11 Margarita Robles-Carrillo, "Digital Identity: An Approach to Its Nature, Concept, and Functionalities," *International Journal of Law and Information Technology* 32, no. 1 (2024): 1, https://doi.org/10.1093/ijlit/eaae019.

recognizably distinct existence.[12] Identity is an interdisciplinary issue with political and cultural dimensions that are important from the perspective of legal sciences, especially in the area of human rights.[13] This discussed electronic user authentication solution enables public services to be provided at a distance in a secure, fast, and comprehensive manner, including in the areas of telemedicine and eHealth. It eliminates unnecessary visits to a healthcare provider that are motivated by formal and legal, rather than medical, reasons.

ISO 27002 defines the purpose of identity management as enabling the unique identification of individuals and systems accessing the organization's information and other associated assets, and enabling the appropriate assignment of access rights.[14] It should be noted that, in information technologies, entities with an identity include not only individuals, but also ICT systems and their web services.

In information technology, identification is understood as the process of establishing someone's identity. According to Article 3(1) of the eIDAS,[15] electronic identification means the process of using data in electronic form that uniquely identifies a person or uniquely represents a specific entity (a natural person or legal entity, or a natural person representing a legal entity).

Electronic identity management solutions enable the secure, efficient, and automated management of access to eHealth systems and the resources within them.[16] This makes it possible to further exploit the potential of these tools to improve healthcare quality, while guaranteeing the rights of data subjects and individuals who are recipients of the electronic services offered.

4. EU Legal Solutions

The primary piece of EU legislation on electronic identity is the eIDAS Regulation. From the perspective of the article's subject matter, it regulates electronic signatures, electronic seals, and associated certificates. These solutions are based on electronic data that are attached to, or logically associated with, other electronic data, and which are used by the performer of these activities to ensure the realization of information security attributes, such as authenticity, non-repudiation, accountability, and integrity. The processes

12 *ISO/IEC 24760–1 – Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology* (Geneva: ISO, 2025), 1.

13 Bartosz Liżewski, "The Personal Identity of the Human Being and the Right to Privacy from the Perspective of Standards of the European Court of Human Rights: Theoretical Legal Reflections," *Bialystok Legal Studies* 29, no. 3 (2024): 78–79, https://doi.org/10.15290/bsp.2024.29.03.05.

14 *ISO/IEC 27002 – Information security, cybersecurity and privacy protection – Information security controls* (Geneva: ISO, 2022), 29.

15 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 (OJ L 257/73, 28 August 2014).

16 As a part of the technical standards of IHE profiles – recommended in the European Commission decision 2015/1302 of 28 July 2015 on the identification of "Integrating the Healthcare Enterprise" profiles for referencing in public procurement – The Patient Identifier Cross-referencing HL7 Integration Profile (PIXV3) is targeted at cross-enterprise Patient Identifier Cross-reference Domains as well as healthcare enterprises with developed IT infrastructure ("Patient Identifier Cross-referencing HL7 V3 (PIXV3)," Integrating the Healthcare Enterprise, August 4, 2023, accessed February 25, 2026, https://profiles.ihe.net/ITI/TF/Volume1/ch-23.html).

described here, therefore, allow the identity of the entity performing such actions to be declared and reliably confirmed. A certificate is an electronic credential that associates the data used to validate a signature or electronic seal with the entity that uses it. These solutions are, therefore, used to identify natural persons (patients and health professionals) and legal entities (healthcare providers) based on the activities they carry out.

It is worth mentioning that electronic certificates can be used not only to certify the identity of natural persons or legal entities, but also, thanks to the Secure Socket Layer/Transport Layer Security protocol, to ensure the authenticity of websites and web services, as well as the integrity and confidentiality of communications via these solutions. The data structures contained in the certificates in question are mostly compliant with the X.509 standard.[17] The technologies presented here create an interoperable environment for managing electronic identity data.

Cross-border health care using eHealth solutions requires effective methods to manage the identity of those who use them. Activities related to the promotion of universal methods for identifying and authenticating users of healthcare information systems are among the objectives pursued by the eHealth Network, established under Article 14 of Directive 2011/24/EU. One activity undertaken by this consultative and advisory EU body involves issuing recommendations concerning the application of the eIDAS Regulation and eIDs in day-to-day healthcare operations, as well as the use of public registers of persons performing healthcare activities.[18]

In the Regulation 2025/327 on the European Health Data Space,[19] Article 16 indicates that one of the requirements of a secure and interoperable health data processing environment is to ensure that data users only have access to the electronic health data which they are authorized to access, and only by means of individual and unique user identities and confidential modes. Moreover, regarding medical professionals using priority categories of electronic personal health data (patient summaries, electronic prescriptions and dispensations, medical imaging studies, and related imaging reports), the requirements for their use of eIDAS-compliant electronic identification means are set out in Article 12 of the EHDS. Ensuring accountability for access to medical databases should be based on effective, legally recognized user authentication mechanisms that guarantee the realization of fundamental rights, such as privacy and the informational autonomy of the individual.

It should be added that the introduction of the legal act under consideration is to be coupled with the implementation of data controller obligations related to the implementation of new mechanisms for the electronic identification of patients, health professionals,

---

17 Diana Gratiela Berbecaru and Antonio Lioy, "An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem," *IEEE Access* 11 (2023): 79160, https://doi.org/10.1109/ACCESS.2023.3299357.

18 European *eHealth Network*, *Recommendation Paper on Policies Regarding eIDAS eID and Health Professional Registries* (Brussels: European *eHealth Network*, May 15, 2018), accessed June 3, 2025, https://health.ec.europa.eu/system/files/2018-09/ev_20180515_co11b_en_0.pdf.

19 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L 327, 5 March 2025).

and researchers, including in relation to the digital identity wallet.[20] The concepts for new regulations in this area were laid out in the eIDAS amendment, which extended harmonization and improved the security of trust services.[21] Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024, amending Regulation No. 910/2014 as regards establishing the European Digital Identity Framework,[22] introduces a normative definition of the concept of a European Digital Identity Wallet, which is a product and service that enables a user to store identity data, credentials, and attributes associated with their identity, provide them on demand to relevant parties, and use them for online and offline authentication.[23] The presented solution is a universal, secure, and reliable tool for managing personal electronic identification facilities.[24]

The dispersion of eID regulation across the EU internal market and healthcare legislation creates a significant risk of inconsistencies in the normative solutions established. The eHealth Network, Data Protection Authorities, and ENISA have a particular role in flagging potential gaps and conflicts to ensure the cybersecurity of solutions introduced and subsequently applied throughout their lifecycle.

5. Patient Rights and Electronic Identification in Healthcare

The patient's right to health services in accordance with current medical knowledge also includes the use of modern techniques for the electronic processing of medical data, in particular for teleconsultation or diagnostic imaging.[25] Electronic identity has a significant impact on increasing the accessibility of eHealth systems for people with reduced mobility, hearing, or visual impairments. It is impossible not to mention here Directive 2016/2102,[26] the implementation of which in the legal order of EU Member States creates the necessary legal requirements in the area under consideration, which also apply to a significant part of healthcare entities. Their adoption by healthcare providers in the EU is

[20] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, recital 21.

[21] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, COM(2021) 281 final (Brussels, June 3, 2021), 281.

[22] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L 1183, 30 April 2024).

[23] In Poland, the adoption of the European digital identity wallet concept was proposed in a draft bill amending the Act on Trust Services and Electronic Identification and certain other acts (RCL No. UC122 of 18 February 2026).

[24] Julián Inza, "The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation," in *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*, ed. Carmen Pastor Sempere (Cham: Springer, 2025), 440.

[25] Dorota Karkowska, "Prawo pacjenta do świadczeń zdrowotnych (art. 6)," in *Prawa pacjenta i Rzecznik Praw Pacjenta. Komentarz*, ed. Dorota Karkowska (Warsaw: Wolters Kluwer, 2021), 232–392.

[26] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2 December 2016).

often insufficient.[27] Solutions that implement digital accessibility standards (e.g., the Web Content Accessibility Guidelines) in eHealth systems can offer better-tailored access to health information and medical records, including diagnostic test results.[28]

Dynamic adaptation of user access conditions in specific data-processing circumstances is possible due to the layering (content, structure, and visualization) and modularity of electronic documents (division into sections), which are completely independent of the medium (data storage) on which they are processed. A document can therefore be dynamically divided into sections without affecting its structure. This facilitates the visualization of individual sections adapted to the specific recipient. It is also possible to hide certain information from a user who lacks the necessary rights to access it lawfully.

Using digital identity solutions, patients can consent to both telemedicine and traditional services. This makes it easier to read the information about the procedure and allows such a statement of intent to be expressed anywhere, anytime. The patient is not obliged to collect the relevant paper form in advance and, once signed, to physically deliver it before the medical procedure begins.

The patient's right to health information and the right of access to electronic records can be realized through ICT. They are significantly intertwined in terms of subject matter (information) and object (patients and health professionals). The right to medical records is the de facto basis for the realization of the right to health information, as it serves as the designated collection of patient data regarding the treatment process.[29] These rights guarantee an appropriate degree of autonomy and subjectivity to the patient, and enable him to make genuinely voluntary decisions in healthcare.[30] The right of access to medical records and the right to be informed about one's health facilitate informed consent, understood as an informed act, made by the patient or the patient's legal representative, freely chosen and clearly expressed, based on coherent, reliable information about all stages of the medical procedure.[31] A person who is comprehensively and precisely informed about their health condition can become an aware participant in healthcare processes.

Electronic identity, in the context of the right to privacy and the physician–patient privilege, enables the confidentiality of patient-related information. This assumption is made possible by pursuing authenticity and accountability as part of data processing activities. Methods for identifying, authenticating, and authorizing users of eHealth and EHR systems enable the recording of which actions have been performed and when.

---

27 Marika Jonsson et al., "How Have Public Healthcare Providers in Sweden Conformed to the European Union's Web Accessibility Directive Regarding Accessibility Statements on Their Websites?," *Universal Access in the Information Society* 24 (2025): 456, https://doi.org/10.1007/s10209-023-01063-1.

28 Gloria Acosta-Vargas et al., "Improvement of Accessibility in Medical and Healthcare Websites," in *Advances in Human Factors and System Interactions: Proceedings of the AHFE 2021 Virtual Conference on Human Factors and Systems Interaction, July 25–29, 2021, USA*, ed. Isabel L. Nunes (Cham: Springer, 2021), 266–73.

29 Izabela Bernatek-Zaguła, *Prawo pacjenta w Polsce do informacji medycznej* (Toruń: Wydawnictwo Adam Marszałek, 2008), 93.

30 Tomasz Pietrzykowski and Katarzyna Smilowska, "The Reality of Informed Consent: Empirical Studies on Patient Comprehension – Systematic Review," *Trials* 22, no. 57 (2021): 7–8, https://doi.org/10.1186/s13063-020-04969-w.

31 Małgorzata Świderska, *Zgoda Pacjenta na zabieg medyczny* (Toruń: Dom Organizatora TNOiK, 2007), 19.

If these processes fail, an unauthorized person should not have access to the protected resources. The use of adequate safeguards to address a constantly evolving catalog of threats is particularly important for protecting data processed in healthcare using ICT.[32] It is worth noting that access control is one of the areas indicated in ISO 27001 requirements for Information Security Management Systems.[33] The use of appropriately clear and effective legal and technical mechanisms to restrict access to patient data only to genuinely justified cases of use, taking into account the necessity and proportionality of the measures taken, should be the standard for managing processable resources in the health information system.[34] With regard to medical confidentiality, the user authentication mechanisms discussed here help protect the patient's autonomy by effectively identifying those authorized to access their health data. The right to informational self-determination through the use of the technical and organizational access management solutions discussed here can be adequately preserved in this case.[35] Effective data exchange in healthcare that guarantees confidentiality, integrity, authenticity, non-repudiation, and accountability is an important factor in ensuring that the quality of services provided meets the needs while maintaining the level of trust in the doctor–patient relationship.

The use of properly functioning electronic services for the management of user identity in e-Health systems is closely linked to the respect of patient rights. This allows these legal obligations to be implemented in the electronic processing of medical data and to ensure an appropriate degree of autonomy for data subjects.

6. The Estonian Electronic Identification System

At the beginning of the 21st century, Estonia's information infrastructure for electronic data processing was among the best developed in Europe.[36] Its foundation is X-Road – an ICT environment for unified and secure data exchange between private and public-sector organizations across the country.[37] Part of the nationwide information infrastructure is the Estonian Electronic Identification System (e-ID), consisting of the following elements:

– ID card (chapter 5 "Identity Card" – § 19 – § 20),
– Residence Permit card (chapter 7 "documents held by aliens" – § 34^1 – § 34^3),

[32] Bożena Skubis, "Ochrona danych medycznych w okresie pandemii COVID-19. Działania Rzecznika Praw Pacjenta dotyczące prawa do dokumentacji medycznej i tajemnicy informacji w latach 2020–2022," *Przegląd Prawa Medycznego* 6, no. 3 (2024): 61, https://doi.org/10.70537/vmgpq521.

[33] *ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (Geneva: ISO, 2022), 12.

[34] Robert Pudlo, Małgorzata Pudlo, and Marcin Burdzik, "Medical Confidentiality in the Polish Legal System: A Real or Illusory Instrument of Patient Privacy Protection?," *Psychiatria Polska* 58, no. 5 (2024): 902–03, https://doi.org/10.12740/pp/onlinefirst/166174.

[35] Sabine Michalowski, *Medical Confidentiality and Crime* (Aldershot: Ashgate, 2003), 12–13.

[36] Edwin Bendyk, "Web 2.0 – sposób na modernizację administracji z udziałem obywateli," *Elektroniczna Administracja*, no. 1 (2008): 53.

[37] Karoline Paide et al., "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," in *ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, eds. Atreyi Kankanhalli, Adegboyega Ojo, and Delfina Soares (New York: ACM, 2018), 34.

- Digi-ID (chapter 5^1 "Digital Identity Card" – § 20^1 – § 20^3),
- e-Residency Digi-ID (chapter 5^2 "e-Resident's Digital Identity Card" – § 20^5 – § 20^{12}),
- Mobiil-ID (chapter 5^1 "Digital Identity Card" – § 20^3 – § 20^4),
- Diplomatic identity card (chapter 5^3 "Diplomatic Identity Card" – § 20^{13} – § 20^{16}).

The functionalities described are widely used in the domestic legal environment, not only to identify individuals and determine their eligibility for health insurance and access to health services or medical records, but also for administrative procedures, public registers, banking services, public transport, social benefits, and general elections (voting).[38] The legal basis for these solutions is the Identity Documents Act (Estonian: *Isikut tõendavate dokumentide seadus*) passed in 1999.[39] The concept of electronic identity corresponds most closely to Digi-ID. This tool allows a specific person to be identified solely in an electronic (digital) environment and thus to use the assigned services.[40] In other cases, we are in fact dealing with hybrid solutions that can be used for analogue, stationary activities (Information System Authority, ID card). It should be added that the Health Services Organisation Act (Estonian: *Tervishoiuteenuste korraldamise seadus*), applied since 2002, implies the use of the e-ID solutions for healthcare (chapter 5^1 "Health Information System" – § 59^1 – § 59^4).[41]

An interesting solution is Mobiil-ID, which verifies a person's identity using the mobile device and the data stored on its SIM card (Information System Authority, Mobile-ID). This method of identification bears similarities to the Polish system for identifying people via the *mObywatel* (mCitizen) application, which will be described in more detail later in this article.

The electronic identity solutions described are used within the Estonian healthcare system, which relies heavily on ICT. The e-Health solutions operating in Estonia are among the most mature in the European Union, as evidenced by the implementation of electronic access services for citizens, categories of accessible health data, access technologies, and coverage and access opportunities for certain categories of people.[42] According to data from as early as 2011, 84% of prescriptions generated under this system were electronic.[43] In addition to this functionality, the national eHealth system (Estonian: *Terviseportaal*) also enables enrolment in health services, access to patients' medical records, teleconsultation, and full processing of laboratory test and diagnostic imaging

38 Kamil Czaplicki, *Dokumenty tożsamości. Jawność i bezpieczeństwo* (Warsaw: C.H. Beck, 2016), 310.

39 It also includes rules on travel documents (chapter 6), including Estonian citizens' passports (§ 21). In Poland, this issue is covered by a special law of January 27, 2022 on passport documents (Journal of Laws 2024, item 1063).

40 Piia Tammpuu et al., "Estonian e-Residency and Conceptions of Platform-Based State Individual Relationship," *Trames Journal of the Humanities and Social Sciences* 26, no. 1 (2022): 7, https://doi.org/10.3176/tr.2022.1.01.

41 In Poland, the rules governing the operation of national e-Health systems are set out separately in the Act on the healthcare information system.

42 Estonia achieved a 100% score in the 2024 eHealth maturity scores report and ranked first. Poland, with a score of 92%, ranked sixth (Martin Page and Puck de Waal, *2025 Digital Decade eHealth Indicator Study: Executive Summary* [Luxembourg: Publications Office of the European Union, 2025], 8, https://data.europa.eu/doi/10.2759/0682933).

43 Taavi Lai et al., "Estonia: Health System Review," *Health Systems in Transition* 14, no. 6 (2013): 103.

data.[44] The wide range of functionality, along with consistency and interoperability with other electronic services, including e-ID, puts the Estonian health care information system at the forefront in Europe in terms of the development and comprehensive use of ICT capabilities.

7. Electronic Identification Solutions in Poland

The Polish Public Electronic Identification System, until April 19, 2023, includes two means of identification: a trusted profile (Polish: *Profil Zaufany*) and a personal profile (Polish: *Profil Osobisty*).[45] Pursuant to Article 3, point 14 of the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks,[46] the trusted profile contains data that identifies and describes a natural person, which was issued in accordance with the provisions of the law, while pursuant to Article 2, paragraph 1, point 10 of the Act of 6 August 2010 on identity cards,[47] the personal profile includes data confirmed by a certificate, which is an electronic attestation used to identify and authenticate the holder of an identity card confirming the data of that person. These solutions can be used in user authentication for services within the healthcare information system, such as the Internet Patient Account (Polish: *Internetowe Konto Pacjenta*, pacjent.gov.pl)[48] and eGabinet (gabinet.gov.pl) for medical professionals.

mCitizen (Polish: *mObywatel*) is a mobile application that provides electronic documents as digital services. An *mObywatel* document is a mobile document (i.e., an electronic document supported by a service made available through the *mObywatel* application) confirming the identity and citizenship of Poles and other residents. The legal basis for this means of identification is the Act of 26 May 2023 on the *mObywatel* application.[49] Although this service, as a rule, can only be used in traditional, stationary contacts with medical entities, the identification data is in electronic form. Moreover, an *mObywatel* profile is a designated authentication tool for users of public ICT systems.

De lege ferenda, efforts should be made to integrate these Polish Public Electronic Identification System services with both the electronic delivery system[50] and mo-

44 Kaija Kasekamp et al., "Estonia: Health System Review," *Health Systems in Transition* 25, no. 5 (2023): 26.

45 Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ C 2836, 22 April 2024).

46 Act on the computerization of the activities of entities performing public tasks of 17 February 2005, Journal of Laws 2024, item 1557.

47 Act on identity cards of 6 August 2010, Journal of Laws 2022, item 671.

48 It should be noted that the electronic Health Insurance Card provided for in Article 49 of the Act of 27 August 2004 on healthcare services financed from public funds (Journal of Laws 2024, item 146), which could potentially be used to identify patients in the healthcare system, is not currently being issued (Andrzej Sidorko, "Karta ubezpieczenia zdrowotnego i inne dokumenty potwierdzające prawo do świadczeń [art. 49]," in *Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Komentarz*, ed. Agnieszka Pietraszewska-Macheta, 4th ed. [Warsaw: Wolters Kluwer, 2023], 491–93, LEX/el).

49 Act on the *mObywatel* application of 26 May 2023, Journal of Laws 2024, item 1275.

50 The issue of exchange of correspondence with public entities in Poland is comprehensively regulated by the Act of 18 November 2020 on electronic delivery (Journal of Laws 2024, item 1045). The electronic registered delivery service provided for therein is a trust service within the meaning of eIDAS. The proper functioning

bile *mObywatel* services, so that they are consistent in terms of legal construction and technical requirements, and do not raise doubts about their interoperability and scope of application. The public identification services operating in Poland – unlike in Estonia – are characterized by too much dispersion and are not fully compatible.

8. Conclusions

The use of electronic data processing technologies is becoming widespread. In addition to their collection, editing, and reading, they are increasingly subject to complex statistical analyses and are becoming a resource for Machine Learning and Artificial Intelligence algorithms. These challenges also apply to the healthcare system. The aging of European populations and the resulting growing demand for healthcare services, coupled with a lack of medical professionals relative to current needs, make the use of eHealth solutions indispensable for maintaining the quality of healthcare services. The increasing interoperability and potential for using information resources in this sector are closely correlated with the development of evidence-based medicine.

In an ever more digitalized world, electronic identity management mechanisms are becoming more important, including in healthcare, which is increasingly using eHealth systems to deliver healthcare services. The legal solutions in this area are still being optimized to address the technical and social challenges of the coming decades. During this process, it is crucial to ensure the privacy and information autonomy of individuals, while exploiting the full potential of modern data processing techniques – without unjustifiably interfering with fundamental rights. These processes are carried out to extract as much useful information as possible, as well as a range of valuable knowledge from these resources, to understand better the reality around us, especially with respect to healthcare and support for decision-making.

The issue of user identification in eHealth systems, discussed in this article, concerns the authentication process, which verifies the identity of the specific person. Establishing the user's identity allows, as part of the next authentication phase, to allocate them a range of access to protected information resources, commensurate with their level of privileges in the ICT system. This therefore allows the legal requirements related to the protection of personal data and the secrets of the medical profession from unauthorized access by unauthorized persons to be realized.

In the case of the methods used to identify individuals in Estonia, a logical division has been adopted between physical identity documents with an electronic layer (ID cards) and digital identities (Digi-ID), and mobile profiles (Mobiil-ID), operated exclusively in electronic form, the latter via mobile devices. A similar concept has been adopted in Poland, assuming the existence of an identity card with an electronic personal profile, a trusted profile and an m-Citizen profile. However, regulations concerning electronic identification in Poland are scattered across many legal acts (the ID Card Act, the Computerisation Act, the *mObywatel* Application Act, the Electronic Delivery Act).

of health care is based not only on the implementation of clinical activities, but also on effective management processes involving interactions with public entities.

In Estonia, on the other hand, this issue has been unified in a single act, the Identity Documents Act. In addition, the national Public Electronic Identification System, which complies with the requirements of Article 9(1) of eIDAS, consists of all the comprehensive methods of authenticating natural persons in Estonia mentioned in this article (ID card, RP card, Digi-ID, e-Residency Digi-ID, Mobiil-ID, Diplomatic identity card), while in Poland it consists only of Trusted profile and Personal profile (linked to the Identity Card), without including the identification functionality in the *mObywatel* application. The Estonian approach, which assumes uniformity of the solutions adopted – both in the sphere of legal instruments and technical solutions – is more coherent and mature. This consideration applies to both the normative and technical/implementation layers, based on the integration of electronic identification services.

The proper functioning of health care based on electronic data processing and eHealth requires secure, trusted user identity management services and proven mechanisms for managing access to protected health information resources. The importance of consistent and effective regulation in this area, supported by non-legal instruments such as technical standards and soft law – especially internal organizational policies and codes of conduct – cannot be overstated.

References

Acosta-Vargas, Gloria, Patricia Acosta-Vargas, Janio Jadán-Guerrero, Luis Salvador-Ullauri, Mario Gonzalez. "Improvement of Accessibility in Medical and Healthcare Websites." In *Advances in Human Factors and System Interactions: Proceedings of the AHFE 2021 Virtual Conference on Human Factors and Systems Interaction, July 25–29, 2021, USA*, edited by Isabel L. Nunes, 266–73. Cham: Springer, 2021.

Bendyk, Edwin. "Web 2.0 – sposób na modernizację administracji z udziałem obywateli." *Elektroniczna Administracja*, no. 1 (2008): 53.

Berbecaru, Diana Gratiela, and Antonio Lioy. "An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem." *IEEE Access* 11 (2023): 79156–75. https://doi.org/10.1109/ACCESS.2023.3299357.

Bernatek-Zaguła, Izabela. *Prawo pacjenta w Polsce do informacji medycznej*. Toruń: Wydawnictwo Adam Marszałek, 2008.

Coggon, John, and José Miola. "Autonomy, Liberty, and Medical Decision-Making." *Cambridge Law Journal* 70, no. 3 (2011): 523–47.

Czaplicki, Kamil. *Dokumenty tożsamości. Jawność i bezpieczeństwo*. Warsaw: C.H. Beck, 2016.

Drozdowska, Urszula, Ewa Kowalewska-Borys, Arkadiusz Bieliński, and Wojciech Wojtal. *Dokumentacja medyczna*. Warszawa: Eskulap, 2011.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*. COM(2008) 689 final. Brussels, November 4, 2008.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. COM(2021) 281 final. Brussels, June 3, 2021.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*. COM(2022) 197 final. Brussels, May 3, 2022.

European *eHealth Network*. *Recommendation Paper on Policies Regarding eIDAS eID and Health Professional Registries*. Brussels: European *eHealth Network*, May 15, 2018. Accessed June 3, 2025. https://health.ec.europa.eu/system/files/2018-09/ev_20180515_co11b_en_0.pdf.

Integrating the Healthcare Enterprise. "Patient Identifier Cross-Referencing HL7 V3 (PIXV3)," August 4, 2023. Accessed February 25, 2026. https://profiles.ihe.net/ITI/TF/Volume1/ch-23.html.

Inza, Julián. "The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation." In *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*, edited by Carmen Pastor Sempere, 433–52. Cham: Springer, 2025.

ISO 27799 – Health informatics – Information security controls in health based on ISO/IEC 27002. Geneva: ISO, 2025.

ISO/IEC 24760–1 – Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology. Geneva: ISO, 2025.

ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022.

ISO/IEC 27002 – Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022.

Jonsson, Marika, Catharina Gustavsson, Jan Gulliksen, and Stefan Johansson. "How Have Public Healthcare Providers in Sweden Conformed to the European Union's Web Accessibility Directive Regarding Accessibility Statements on Their Websites?." *Universal Access in the Information Society* 24 (2025): 449–62. https://doi.org/10.1007/s10209-023-01063-1.

Karkowska, Dorota. "Prawo pacjenta do świadczeń zdrowotnych (art. 6)." In *Prawa pacjenta i Rzecznik Praw Pacjenta. Komentarz*, edited by Dorota Karkowska, 232–392. Warsaw: Wolters Kluwer, 2021.

Kasekamp, Kaija, Triin Habicht, Andres Võrk, Kristina Köhler, Marge Reinap, Kristiina Kahur, Heli Laarmann, and Yulia Litvinova. "Estonia: Health System Review." *Health Systems in Transition* 25, no. 5 (2023): 1–236.

Lai, Taavi, Triin Habicht, Kristiina Kahur, Marge Reinap, Raul Kiivet, Ewout van Ginneken. "Estonia: Health System Review." *Health Systems in Transition* 14, no. 6 (2013): 1–196.

Liżewski, Bartosz. "The Personal Identity of the Human Being and the Right to Privacy from the Perspective of Standards of the European Court of Human Rights: Theoretical Legal Reflections." *Bialystok Legal Studies* 29, no. 3 (2024): 77–90. https://doi.org/10.15290/bsp.2024.29.03.05.

Maj, Zuzanna. "Elektroniczna dokumentacja medyczna – wybrane aspekty prawne." *Przegląd Prawa Medycznego* 4, no. 1 (2022): 121–22. https://doi.org/10.70537/14y42909.

Michalowski, Sabine. *Medical Confidentality and Crime*. Aldershot: Ashgate, 2003.

Muzaik, Suhail, and Nadia Davoody. "Exploring the Operational and Technical Changes in the Healthcare Sector During the COVID-19 Pandemic." In *Telehealth Ecosystems in Practice*, edited by Mauro Giacomini et al., 277–81. Amsterdam: IOS Press, 2023.

Page, Martin, and Puck de Waal. *2025 Digital Decade eHealth Indicator Study: Executive Summary*. Luxembourg: Publications Office of the European Union, 2025. https://data.europa.eu/doi/10.2759/0682933.

Paide, Karoline, Ingrid Pappel, Heiko Vainsalu, and Dirk Draheim. "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships." In *ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, edited by Atreyi Kankanhalli, Adegboyega Ojo, and Delfina Soares, 34–41. New York: ACM, 2018.

Pietrzykowski, Tomasz, and Katarzyna Smilowska. "The Reality of Informed Consent: Empirical Studies on Patient Comprehension – Systematic Review." *Trials* 22, no. 57 (2021): 7–8. https://doi.org/10.1186/s13063-020-04969-w.

Pudlo, Robert, Małgorzata Pudlo, and Marcin Burdzik. "Medical Confidentiality in the Polish Legal System: A Real or Illusory Instrument of Patient Privacy Protection?." *Psychiatria Polska* 58, no. 5 (2024): 895–907. https://doi.org/10.12740/pp/onlinefirst/166174.

"Raport z badania satysfakcji pacjentów korzystających z teleporad u lekarza podstawowej opieki zdrowotnej w okresie epidemii COVID-19" (2020). Accessed June 4, 2025. https://www.gov.pl/attachment/a702e12b-8b16-44f1-92b5-73aaef6c165c.

Robles-Carrillo, Margarita. "Digital Identity: An Approach to Its Nature, Concept, and Functionalities." *International Journal of Law and Information Technology* 32, no. 321 (2024): eaae019. https://doi.org/10.1093/ijlit/eaae019.

Sidorko, Andrzej. "Karta ubezpieczenia zdrowotnego i inne dokumenty potwierdzające prawo do świadczeń (art. 49)." In *Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Komentarz*, edited by Agnieszka Pietraszewska-Macheta, 4th ed., 491–93. Warsaw: Wolters Kluwer, 2023. LEX/el.

Skubis, Bożena. "Ochrona danych medycznych w okresie pandemii COVID-19. Działania Rzecznika Praw Pacjenta dotyczące prawa do dokumentacji medycznej i tajemnicy informacji w latach 2020–2022." *Przegląd Prawa Medycznego* 6, no. 3 (2024): 50–74. https://doi.org/10.70537/vmgpq521.

Świderska, Małgorzata. *Zgoda Pacjenta na zabieg medyczny*. Toruń: Dom Organizatora TNOiK, 2007.

Tammpuu, Piia, Anu Masso, Mergime Ibrahimi, and Tam Abaku. "Estonian e-Residency and Conceptions of Platform-Based State Individual Relationship." *Trames Journal of the Humanities and Social Sciences* 26, no. 1 (2022): 3–21. https://doi.org/10.3176/tr.2022.1.01.

World Health Organization. Eastern Mediterranean Region. "eHealth." Accessed June 4, 2025. https://www.emro.who.int/health-topics/ehealth/.