UNIWERSYTET ZIELONOGÓRSKI

DYSKURS PRAWNICZY I ADMINISTRACYJNY 2/2026 ISSN 2657-926X

Agnieszka Jankowska
Fundacja Digital Poland
Ministerstwo Cyfryzacji
ORCID: 0009-0001-8423-5426
agnieszka.jankowska1@op.pl

Cybersecurity Standards in Public Health. Regulatory and Systemic Challenges in the Era of Data-driven Healthcare

Keywords: cybersecurity, public health, health data, digital regulation

Summary. The article examines cybersecurity in public health in the context of the dynamic development of digital technologies and the growing role of health data as a strategic resource. The starting point is the assumption that despite numerous legal regulations, technical standards and guidelines at the national and EU levels, the healthcare system operates in conditions of significant regulatory and organizational fragmentation. The varying levels of digital maturity among healthcare entities, limited financial and human resources and insufficient implementation coordination translate into a fragmented and inconsistent approach to cyber risk management. The article discusses the importance of health data for the innovation and competitiveness of the European Union and identifies key cyber threats in the healthcare sector. The conclusion presents directions for systemic change, pointing to the need for a more integrated regulatory model combining legal, technical and organizational standards with investments in competencies, infrastructure and building institutional resilience.

Standardy cyberbezpieczeństwa w zdrowiu publicznym. Wyzwania regulacyjne i systemowe w erze opieki zdrowotnej opartej na danych

Słowa kluczowe: cyberbezpieczeństwo, zdrowie publiczne, dane zdrowotne, regulacje cyfrowe

Streszczenie. Artykuł analizuje problematykę cyberbezpieczeństwa w zdrowiu publicznym w kontekście dynamicznego rozwoju technologii cyfrowych oraz rosnącej roli danych zdrowotnych jako strategicznego zasobu. Punktem wyjścia jest założenie, że mimo licznych regulacji prawnych, norm technicznych i wytycznych na poziomie krajowym i unijnym, system ochrony zdrowia funkcjonuje w warunkach znacznego rozproszenia regulacyjnego i organizacyjnego. Zróżnicowany poziom dojrzałości cyfrowej podmiotów leczniczych, ograniczone zasoby finansowe i kadrowe oraz niedostateczna koordynacja wdrożeń przekładają się na fragmentaryczne i niespójne podejście do zarządzania ryzykiem cybernetycznym. Artykuł omawia znaczenie danych zdrowotnych dla innowacji i konkurencyjności Unii Europejskiej, a także identyfikuje kluczowe zagrożenia cybernetyczne w sektorze ochrony zdrowia. W konkluzji przedstawiono pożądane kierunki zmian systemowych, wskazując na potrzebę bardziej zintegrowanego modelu regulacyjnego, łączącego standardy prawne, techniczne i organizacyjne z inwestycjami w kompetencje, infrastrukturę i budowę odporności instytucjonalnej.

1. Introduction: The Data Era

Technological progress, accompanied by the pervasive digitalization of social, economic and administrative processes, has resulted in the exponential growth of data generated, processed and stored in the digital form. The contemporary data ecosystem is characterized not only by quantitative expansion, but by qualitative transformation as well: data has become a strategic resource underpinning innovation, automation and decision-making across both public and private sectors. The global volume of data is increasing at an unprecedented pace, driven primarily by the rapid deployment of artificial intelligence, the expansion of the Internet of Things (IoT), widespread adoption of cloud computing and the ongoing digital transformation of industries and public services.

According to the latest estimates from Statista.com reports, the global volume of data reached 149 zettabytes in 2024 and is projected to grow to 181 zettabytes by the end of 2025[1]. On a daily basis hundreds of millions of terabytes of data are generated worldwide (throughout 2024 approximately 402.74 million terabytes of data were generated every day) and recent analyses suggest that the volume of stored data doubles roughly every four years[2]. This dynamic reflects the deepening digitization of global activities, encompassing consumer services, industrial production, healthcare, finance, public administration and critical infrastructure. At the same time, it exposes structural limitations in existing data storage architectures, cybersecurity mechanisms and governance frameworks.

Artificial intelligence plays a central role in this process. Machine learning models, large language models and generative AI systems generate and process vast datasets during both training and deployment phases. Applications such as automated content generation, recommendation systems, predictive analytics and decision-support tools rely on continuous data inflows and feedback loops to optimize performance. This constant circulation of data not only amplifies data volumes but also increases legal and technical risks related to data integrity, confidentiality and accountability, particularly where AI systems operate on sensitive or high-risk datasets. A significant proportion of global data production originates from digital platforms, especially social media ecosystems. Platforms facilitating user-generated content, such as video-sharing, image-based and short-form content services, handle billions of uploads and interactions daily. Each user action contributes to expanding pools of structured and unstructured data, while emerging functionalities

[1] https://www.statista.com/statistics/871513/worldwide-data-created/ [accessed on: 01.02.2026].

[2] International Data Corporation, https://www.businesswire.com/news/home/20200513005075/en/IDCs-Global-StorageSphere-Forecast-Shows-Continued-Strong-Growth-in-the-Worlds-Installed-Base-of-Storage-Capacity [accessed on: 02.02.2026].

such as live streaming, immersive media and augmented reality further intensify data generation. Equally important is the role of the Internet of Things, which has transformed everyday objects and industrial equipment into continuous data producers. Smart home systems, wearable health devices, industrial sensors and autonomous or semi-autonomous machines generate real-time data streams that are often processed in distributed and interconnected environments. Additionally, e-commerce and digital service platforms further contribute to the data surge by collecting granular transactional and behavioral information. Searches, clicks, purchases and user reviews generate datasets that feed algorithmic systems for personalization, dynamic pricing and targeted advertising.

The healthcare sector has become one of the most data-intensive domains of the digital economy, encompassing both private and public healthcare systems. The rapid expansion of electronic health records, medical imaging, wearable devices, and real-time patient monitoring has transformed health data into a cornerstone of contemporary healthcare governance and innovation. Market analyses indicate that the global big data in healthcare sector, valued at over USD 27 billion in 2024, is expected to grow dynamically over the coming decade, reflecting the accelerating integration of data-driven technologies into clinical practice, public health management and biomedical research. The Global Big Data in healthcare market is projected to grow by over 18% annually, reaching even USD 75 billion by 2030[3]. Today, the healthcare industry generates nearly one-third of the world's data volumes. According to the World Health Organization, global health data generation reached 2.314 exabytes in 2023, with projections indicating a threefold increase by 2030, which urgently requires solid infrastructure to manage and leverage this expanding digital footprint[4].

The societal potential of health data is considerable. Large-scale health datasets enable earlier and more accurate diagnoses, evidence-based clinical decision-making, improved disease surveillance and more efficient allocation of public healthcare resources. At the same time, the scale and sensitivity of healthcare data bring significant limitations and risks. Health data is inherently personal and often highly sensitive, making it a prime target for cyberattacks, including ransomware incidents, data breaches and integrity manipulation. The increasing reliance on interconnected digital infrastructures, cloud services and AI-driven analytics expands the attack surface and amplifies the potential impact of cybersecurity failures. In public healthcare systems, such incidents may disrupt essential services, undermine

[3] https://www.techsciresearch.com/report/big-data-in-healthcare-market/4009.html [accessed on: 02.02.2026].

[4] J. Thomason, "Data, digital worlds, and the avatarization of health care", *Global Health Journal*, vol. 8, no. 1 (March 2024), p. 2.

public trust and directly endanger patient safety. From a legal and regulatory perspective, the rapid growth of healthcare data exposes structural tensions between innovation, data protection and cybersecurity obligations. Existing legal frameworks often struggle to keep pace with data-intensive technologies, particularly in areas such as secondary use of health data, cross-border data flows, accountability for AI-driven decision-making and cybersecurity standards for critical health infrastructure. Consequently, while the expansion of healthcare data represents a significant opportunity for societal benefit, it simultaneously necessitates robust, sector-specific data governance and cybersecurity regimes capable of addressing the growing risks inherent in data-driven healthcare ecosystems. In this context, cybersecurity becomes no longer merely a technical issue, but of fundamental normative and systemic significance.

The purpose of this article is to analyze cybersecurity standards in public health amid dynamic digitalization and the growing significance of health data. Despite the existence of numerous legal regulations, technical standards and guidelines at both national and European Union levels, the healthcare system operates within a context of substantial regulatory and organizational fragmentation. This fragmentation stems from the multiplicity of healthcare entities, their varying levels of digital maturity, limited financial and human resources, and the absence of coherent coordination in cyber risk management. Concurrently, the rapid expansion of health data processing, driven by advancements in artificial intelligence, personalized medicine, and European data ecosystems, presents substantial opportunities to enhance the quality of healthcare and the European Union's competitiveness. However, this development intensifies the tension between innovative potential and the system's actual capacity to ensure security. The article argues that the current regulatory model, characterized by its inherent complexity, fails to provide an adequate response to the scale and dynamism of cyber threats, which is a challenge that is exacerbated for healthcare entities. This justifies the need to develop a comprehensive approach that integrates legal frameworks, institutional mechanisms, investments in infrastructure and human capital and cohesive implementation standards, thereby enabling the secure utilization of health data as a strategic resource.

2. Health Data as a Strategic Resource: The European Health Data Space

Data constitute the foundation of the modern internet economy, but companies operating in more traditional industries and sectors are also increasingly relying on data to develop their business activities. Today, there is virtually no area of the economy that has not been affected by digital transformation. The scale of data

generation on a daily basis, particularly in the era of rapidly developing artificial intelligence, creates new potential for economies, societies and the global system as a whole. Data-driven innovation can deliver substantial benefits across multiple sectors, including healthcare through improved personalized medicine, transportation through new mobility solutions and environmental protection through contributions to energy transformation. On the one hand, the growing economic and societal potential of data, and on the other, strong competitive pressure from global players based in the United States and China, have motivated the European Commission to develop a comprehensive EU data strategy. According to the European Commission, improved access to and reuse of data could generate social and economic benefits amounting to between 1% and 2.5% of EU GDP. New common rules and data-sharing mechanisms are expected to have a broad impact on the EU economy and society as a whole. Annual savings in the EU healthcare sector alone are estimated at EUR 120 billion, while EU-27 GDP gains by 2028 are projected to reach EUR 270 billion. Furthermore, whereas in 2018 the value of the EU data economy was estimated at EUR 301 billion (2.4% of EU GDP), by 2025 it was assessed to grow to nearly EUR 830 billion, representing approximately 5.8% of EU GDP[5].

Europe seeks to capture the benefits of improved data use through a comprehensive approach to the data economy, aimed at increasing both the use of data and the demand for data-enabled products, services and processes throughout the Single Market[6]. The European Data Strategy is designed to create conditions for enhanced data utilization across the economy and society, while maintaining appropriate control and security mechanisms, particularly with respect to sensitive data and high standards of cybersecurity, privacy and data protection. Two legislative acts form the core pillars of this strategy: the Data Governance Act, which aims to increase trust in voluntary data-sharing mechanisms, and the Data Act, which establishes rules governing who can access and use which data and for what purposes, across the EU. While the former focuses on facilitating data availability and reuse by regulating data intermediaries and governance structures, the latter seeks to ensure fairness in the distribution of value generated from data. Key element of the EU data strategy is the creation of Common European Data Spaces across a number of strategic economic sectors and domains of public interest. These data spaces are intended to make more data available for access and reuse within a trustworthy and secure environment, benefiting European businesses and citizens

[5] https://digital-strategy.ec.europa.eu/en/factpages/data [accessed on: 03.02.2026].

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European strategy for data, COM/2020/66, Brussels, 19.02.2020.

across fourteen sectors. The first and most significant of these is the healthcare sector. Health data offer enormous potential not only for business development, but above all for advancing scientific research and developing innovative methods of disease treatment. Consequently, at the EU level, steps have been taken to establish a framework for a European Health Data Space[7], intended to serve as a critical bridge between health data ecosystems and the development of advanced technologies, including artificial intelligence. This framework is designed to enable data laboratories and AI factories to use anonymized and synthetic datasets within trusted processing environments[8].

The European Health Data Space (EHDS) constitutes the first common EU data space dedicated to a specific sector under the European Data Strategy. In the coming years, the EHDS is expected to significantly affect, inter alia, patients' access to and control over their medical records, the work of hospitals and healthcare professionals, the development of research and innovation based on advanced technologies and the overall functioning of healthcare systems in the Member States, including Poland[9]. It aims to establish a unified framework for the use and exchange of electronic health data across the EU. At the same time, it enables certain categories of data to be reused for purposes of public interest, policymaking and scientific research. This Regulation also introduces a harmonized legal and technical framework for electronic health record systems, fostering interoperability, innovation and the smooth functioning of the internal market. The EHDS is built on three core pillars: (1) empowering individuals to take control of their health data, ensuring immediate and easy electronic access to their personal health information; (2) supporting the use of health data to improve healthcare delivery across the EU, by strengthening data exchange between Member States, avoiding duplication and enabling healthcare providers to access complete patient medical histories, thereby improving treatment outcomes while saving time and resources; and (3) enabling the EU to fully harness the potential of secure data exchange, as well as the primary and secondary use of health data.

As part of these efforts, the EU expects to achieve savings of EUR 5.5 billion over the next decade through improved access to and exchange of health data within the healthcare sector. An additional EUR 5.4 billion in savings may result from

[7] 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, https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng [accessed on: 07.02.2026].

[8] European Commission, *Communication from the Commission to the European Parliament and the Council: European Data Union Strategy – Unlocking Data for Artificial Intelligence*, Brussels, 19 November 2025, COM(2025) 835 final, pp. 7–8.

[9] A. Ryś„Europejska Przestrzeń Danych Dotyczących Zdrowia – nowe wyzwania i możliwości". *Med. Prakt.*, 2025; no. 3, pp. 110–119.

better use of health data in research, innovation and policymaking, contributing to an estimated 20–30% increase in market growth[10]. The EHDS establishes a robust legal framework for the use of health data for scientific research, innovation, public health purposes, and regulatory policymaking. Under clearly defined conditions, researchers, innovators, public institutions and industry actors will gain access to large volumes of high-quality health data. This access is crucial for the development of life-saving treatments, vaccines, and medical devices, as well as for improving access to healthcare and strengthening the resilience of health systems. Responsible and sustainable governance of health data will support innovation and progress in healthcare, although ensuring data security and compliance with personal data protection principles still remains a major challenge. Achieving the objectives of the EHDS will therefore require cooperation, commitment, and adequate infrastructure. Successful implementation of the EHDS depends above all on consistent and uniform application of this Regulation across all Member States, as well as on ensuring interoperability between information systems to enable scale in scientific and commercial activities. A major challenge lies in the significant disparities between Member States, not only in terms of digital infrastructure development, but also in their readiness to adopt innovation. Countries such as Finland, Denmark, and France already offer examples of mature, system-level digital health solutions[11]. Nevertheless, a number of issues still need to be addressed to ensure effective implementation of the EHDS, including the establishment of clear rules fostering a data-sharing culture, allocation of sufficient resources for upskilling healthcare personnel, investment in technical infrastructure, development of procedures and standards ensuring high data quality and interoperability across healthcare providers. Health systems' capacity to contribute high-quality data to the EHDS, to close the loop between primary and secondary data use and to reintegrate research outputs and innovation back into healthcare practice will ultimately determine whether all EU citizens can benefit equally from the system. Cultural differences, varying perceptions of health data sharing and heterogeneous levels of health and digital literacy across and within Member States must not be underestimated, as they necessitate tailored and intensified efforts in education, communication and stakeholder engagement, strengthening public trust in the use of medical data in both clinical practice and research [12].

[10] The impact of the European Health Data Space Regulation and the Open Data Directive on citizens, European Commission, data.europa.eu, Publications Office of the European Union, July 2025.

[11] A. Ryś, *op. cit.*, p. 117.

[12] Implementing the European Health Data Space across Europe, eitHealth, Think Tank, April 2024, https://eithealth.eu/wp-content/uploads/2024/04/EIT_Health_ThinkTank_Implementing_the_ EHDS_across_Europe_23.04.24.pdf [accessed on: 07.02.2026].

3. Regulatory and Standardization Framework for Cybersecurity in Public Health

Cybersecurity in public health in Poland is currently shaped by a multilayered and fragmented regulatory framework, encompassing provisions of medical law, personal data protection law, public administration digitalization, as well as technical and organizational norms and standards. The obligations imposed on healthcare providers and public institutions stem from multiple normative sources, often pursuing different objectives and applying to different scopes. Below, the most significant regulations and standards relevant to cybersecurity in public health are outlined.

3.1. Medical Law as the Foundation for the Protection of Health Information

The primary regulatory domain determining the manner in which information is processed and protected in the healthcare sector is medical law. The Act of 6 November 2008 on Patients' Rights and the Patient Ombudsman establishes the fundamental principle of confidentiality of patient-related information[13]. Article 13 guarantees patients the right to have all information concerning them, including information about their health status, diagnosis and prognosis, kept confidential by persons performing medical professions. Although the Act does not explicitly refer to cybersecurity, it imposes an obligation on healthcare providers to ensure the confidentiality, integrity and availability of patient health information, which, in the context of digital healthcare systems, directly translates into requirements concerning the security of ICT systems.

This regulation is supplemented by the Regulation of the Minister of Health of 6 April 2020 on medical documentation, which specifies detailed rules for the creation, storage, and processing of medical records, including records maintained in electronic form[14]. The Regulation introduces requirements aimed at protecting medical documentation against damage, loss or unauthorized access; however, similarly to the Patients' Rights Act, it leaves considerable discretion as to the choice of specific technical and organizational measures. In particular paragraphs 86–89 of the Regulation impose an obligation to ensure the integrity, reliability and continuous availability of medical documentation, including through access control mechanisms and safeguards against unauthorized modification of data. At the same time, the Regulation does not define minimum cybersecurity standards

[13] Act of 6 November 2008 on Patients' Rights and the Patients' Rights Ombudsman, Journal of Laws 2024, item 581.

[14] Regulation of the Minister of Health of 6 April 2020 on the types, scope and models of medical documentation and the manner of its processing, Journal of Laws 2024, item 798.

nor does it explicitly refer to recognized technical norms, which in practice leads to significant disparities in the level of protection of electronic medical records across healthcare entities.

Of key importance for the digital infrastructure of public healthcare is also the Act of 28 April 2011 on the Healthcare Information System[15]. This Act establishes the framework for the operation of central ICT systems, such as the P1 platform, and regulates data exchange between participants in the healthcare system. While it emphasizes the need to ensure the security of data processed within healthcare information systems, it does not, like other sectoral acts, introduce a uniform and detailed catalogue of minimum cybersecurity requirements applicable to all system participants.

3.2. Personal Data Protection as a Pillar of Health Information Security

A second fundamental regulatory pillar in the area of public health cybersecurity is personal data protection law. Under the General Data Protection Regulation (GDPR)[16], data concerning health are classified as a special category of personal data, implying a heightened standard of protection. Article 32 of GDPR explicitly obliges controllers and processors to implement "appropriate technical and organizational measures" to ensure the security of processing, including system resilience, the ability to restore data availability promptly and regular testing of safeguards. At the national level, the GDPR is complemented by the Act of 10 May 2018 on the protection of personal data[17], which regulates, inter alia, the competences of the President of the Personal Data Protection Office (UODO) as well as domestic supervisory and sanctioning mechanisms. A significant practical development in the application of the GDPR in the healthcare sector is the "Code of Conduct for the Healthcare Sector", approved by the President of the UODO on 11 December 2023[18]. As the second code issued under Article 40 GDPR for this sector and the first applicable to both public and private entities, it constitutes an attempt to specify the general GDPR obligations in the context of healthcare activities.

---

[15] Act of 28 April 2011 on the Information System in Healthcare, Journal of Laws 2023, item 2465, as amended.

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, p. 1, as amended.

[17] Act of 10 May 2018 on the Protection of Personal Data, Journal of Laws 2019, item 1781, as amended.

[18] Code of Conduct for the Health Care Sector adopted pursuant to Article 40 of Regulation (EU) 2016/679, applicable to healthcare providers and data processors, 11 December 2023, https://uodo.gov.pl/pl/file/4525 [accessed on: 06.02.2026].

Although this Code does not constitute universally binding law, its normative and interpretative relevance for health data security standards is substantial, particularly in the context of data controller responsibility. Application of the Code may serve as evidence of compliance with GDPR obligations by controllers and processors (implementation of the accountability principle). The Code provides a set of guidelines aimed at enhancing the level of personal data protection, consistent with GDPR and national legislation, including principles of data processing under Article 5 of GDPR, data pseudonymization, controller obligations, data protection by design and by default, as well as measures ensuring the security of processing.

3.3. State Digitalization and Interoperability of Healthcare Systems

Another regulatory area affecting cybersecurity in public health concerns the digitalization of public administration. The Act of 17 February 2005 on the computerization of entities performing public tasks[19] establishes a general framework for ICT systems used by public entities, including healthcare institutions performing public tasks. The Act introduces obligations to ensure data security and system compliance with specified standards. Particularly important in this context is the Regulation of the Council of Ministers of 21 May 2024 on the National Interoperability Framework (KRI)[20], which defines minimum requirements for ICT systems and electronic information exchange. Although KRI is not dedicated exclusively to the healthcare sector, in practice it establishes a baseline level of security and interoperability for systems used in public healthcare. At the same time, the Regulation remains general in nature and does not fully reflect the specific risks associated with the processing of medical data.

3.4. Cybersecurity as a Horizontal Regulatory Domain

The regulation most directly addressing cybersecurity issues is the Act of 5 July 2018 on the National Cybersecurity System (KSC)[21], which implements the NIS Directive into Polish law. This Act applies, inter alia, to operators of essential services, a category that in certain cases includes healthcare entities. KSC introduces obligations related to risk management, incident reporting and cooperation

[19] Act of 17 February 2005 on Computerisation of Activities of Entities Performing Public Tasks, Journal of Laws 2024, item 307.

[20] Regulation of the Council of Ministers of 21 May 2024 on the National Interoperability Framework, minimum requirements for public registers and electronic information exchange, and minimum requirements for ICT systems, Journal of Laws 2024, item 773.

[21] Act of 5 July 2018 on the National Cybersecurity System, Journal of Laws 2023, item 913, as amended. At the end of January 2026, the Sejm of the Republic of Poland adopted an amendment to this Act and submitted it for signature by the President of the Republic of Poland; however, at the time of writing, the Act had not yet been signed.

with competent cybersecurity authorities. The importance of this framework will increase with the implementation of the NIS 2 Directive[22], which should have been transposed into Polish law by 18 October 2024. NIS 2 expands the scope of regulated entities and significantly strengthens cybersecurity management requirements, explicitly covering many healthcare entities as essential or important entities. From a public health perspective, this entails a substantial reinforcement of legal obligations related to cyber resilience, while simultaneously raising questions regarding regulatory coherence and the practical feasibility of implementation in the healthcare sector.

3.5. Non-binding Standards and Guidelines in the Healthcare Sector

Legal regulations are complemented by technical and organizational standards and guidelines. Of particular relevance are ISO standards, especially ISO 27799, which constitutes a sector-specific extension of ISO/IEC 27001 and addresses information security management in healthcare. This standard reflects the specificity of medical data and clinical processes, offering practical guidance on protecting the confidentiality, integrity, and availability of health information.

At the national level, an important role is played by guidelines issued by the Centre for eHealth (CeZ), particularly those relating to electronic medical record systems (EDM). Although formally non-binding, these guidelines effectively shape technical standards applied by healthcare providers using the national eHealth infrastructure. At the same time, the absence of a uniform, mandatory catalogue of minimum cybersecurity requirements for the entire healthcare sector leads to significant disparities in security levels across entities. At the EU level, an important reference point is provided by recommendations and analyses issued by the European Union Agency for Cybersecurity (ENISA), including documents on cyber hygiene in the health sector[23]. ENISA identifies healthcare as one of the sectors most exposed to cyber threats and highlights good practices related to risk management, staff training and incident response.

An analysis of the applicable regulations and standards demonstrates that cybersecurity in public health is shaped in a fragmented and poorly coordinated manner. Although numerous legal acts, guidelines and technical standards apply

[22] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[23] ENISA – European Union Agency for Cybersecurity, Cyber Hygiene in the Health Sector, September 2025, https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber%20Hygiene% 20in%20the%20Health%20Sector.pdf [accessed on: 06.02.2026].

to the sector, they do not form a coherent and unequivocal system of minimum cybersecurity requirements. The absence of centrally defined, mandatory standards and imposed technical solutions leaves healthcare entities with significant discretion, resulting in uneven levels of protection and difficulties in assessing regulatory compliance. This situation is further exacerbated by limited coordination between sector-specific regulations, horizontal legal instruments and soft law documents, as well as by insufficient financial resources, competency gaps and inadequate cybersecurity training. Consequently, the healthcare system remains particularly vulnerable to cyber incidents, the effects of which may extend beyond personal data breaches and directly threaten the continuity of healthcare services and patient safety.

4. Cybersecurity Threats in the Healthcare Sector and the Healthcare Data Trilemma: Between Value, Utility and Security

For several years now, Poland has been experiencing a steadily increasing number of cyberattacks, placing it among the most frequently targeted EU Member States. At the turn of 2025 and 2026, Polish government institutions were repelling nearly 3,188 attacks per week, significantly more than countries such as the Czech Republic, Austria or Germany[24]. In 2025, the number of reports registered by the CERT Poland exceeded 658,000, representing an increase of nearly 10% compared to 2024 (601,000) and over 70% compared to 2023 (371,000). The number of cybersecurity incidents recorded by CERT Poland in 2025 reached a record level of more than 260,800 incidents, which constitutes an increase of nearly 152% compared to 2024, when 103,400 incidents were recorded, and over 300% compared to 2023, when nearly 80,000 incidents were registered. In 2024, the highest number of incidents was recorded in public administration (1,911 cases), followed by the education sector (579 cases) and the healthcare sector (440 cases). Among the 57 serious incidents recorded in 2024, 44 occurred in the banking and financial market infrastructure sector, 11 concerned the healthcare sector and 2 were related to the transport sector. The number of serious incidents in 2024 increased by 43% compared to 2023[25].

In recent years, the healthcare sector has increasingly become a victim of cyberattacks and at a significantly higher rate than any other critical sector in the European Union. Medical data currently constitute one of the most attractive targets for cybercriminals. Their particular value stems from the fact that they combine

[24] Checkpoint Research, Cybersecurity Report 2026, https://www.checkpoint.com/security-report/ [accessed on: 07.02.2026].

[25] CSIRT NASK (CERT Polska), *Monthly Summary Report No. 4/2025*, December 2025, pp. 5–6; CERT Polska – NASK, *Annual Report on the Activities of CERT Polska 2023*.

information about an individual's health status with identification, financial and insurance data, making them exceptionally useful for various forms of cybercrime. Unlike payment card data, which can be blocked or replaced, medical data are permanent in nature, therefore once stolen, they may be exploited for many years for identity theft, credit fraud, insurance fraud, blackmail or sophisticated phishing attacks. Their potential commercial value should also not be underestimated, particularly in the context of creating behavioral profiles, conducting statistical analyses or generating personalized offers, which further increases interest in these resources among unauthorized actors. At the same time, the ongoing process of digitalization has revolutionized healthcare in recent years, making an increasing number of patient services available online. Examples include the e-prescription and e-referral systems, the implementation of the Internet Patient Account (IKP) and the rapid development of telemedicine. These initiatives demonstrate that modern technologies in medicine create new opportunities and have a tangible impact on doctors' work and patient care, contributing inter alia to improved quality of treatment and time savings for medical staff. Nevertheless, the healthcare system remains at an early stage of building a comprehensive e-health ecosystem. Significant challenges lie ahead, related to the further digitalization of medical services and the intensified development and use of systems based on cutting-edge technologies, including artificial intelligence. In this context, the proper use of such technologies in the provision of healthcare services will be crucial, particularly with regard to ensuring the security of privacy and health data, as the effective functioning of these systems requires the collection and processing of large datasets analyzed, among others, by artificial intelligence algorithms[26].

The attractiveness of the healthcare sector to cybercriminals is further reinforced by the relatively low level of technical and organizational security in many medical institutions. These entities often operate under conditions of chronic underfunding, limited human resources and a shortage of specialized IT personnel, which in practice leads to delays in implementing updates, a lack of systematic threat monitoring and insufficient staff training. As a result, cyberattacks on healthcare facilities are not only frequent but also relatively effective, causing disruptions and delays in the provision of health- and life-saving services[27]. Cybersecurity has thus ceased to be merely an IT issue and has become a systemic and organizational challenge.

[26] P. Kaźmierczyk, D. Lukosek, M. Czarnuch, A. Horyń, *Medical Data in Physicians' Practice: Current State and Desired Changes*, Report of the Network of Physician Innovators, Supreme Medical Chamber (Naczelna Izba Lekarska), 2023, pp. 23–27.

[27] https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_pl [accessed on: 07.02.2026].

At the beginning of 2025, the Centre for eHealth (CeZ) published the results of the eighth edition of the survey on the level of digitalization of entities providing healthcare services. The aim of the survey was to obtain a comprehensive picture of the level of digitalization of healthcare entities, their readiness to create and share electronic medical documentation, their use of modern technologies (including telemedicine and artificial intelligence), as well as to assess needs and barriers in the area of IT, including cybersecurity[28]. The results indicate a decidedly insufficient level of cybersecurity in medical entities. Dedicated cybersecurity teams operate in only 27.5% of healthcare facilities, with a significantly higher prevalence in hospitals (41.1%) than in outpatient care providers (25.8%). Most of these teams consist of no more than five individuals, suggesting limited human resources and organizational capacity for comprehensive management of ICT security. Moreover, many facilities have not implemented even basic security measures: 60% do not monitor vulnerabilities, nearly one in ten lacks antivirus software and fewer than 60% regularly test backup copies and data recovery procedures.

The low prevalence of dedicated cybersecurity teams, combined with their small size, means that many healthcare facilities lack human resources capable of effectively managing cyber risk. With limited internal teams and a small number of specialists, facilities often rely on external service providers, which may raise challenges related to oversight and information security management. Furthermore, as many as 82.1% of surveyed facilities identified insufficient financial resources for IT investments as the main barrier to further digitalization, including cybersecurity, representing a significant increase compared to the previous survey cycle. Cybersecurity activities are most often financed from the entities' own funds (84.8%), less frequently with support from the National Health Fund (NFZ; 35.6%) or EU funds (10.6%). The lack of adequate budgets results in delays in implementing monitoring tools, risk analysis, intrusion detection systems and advanced security solutions, which are crucial from the perspective of cyber resilience. At the same time, the reported needs in the area of cybersecurity confirm that awareness of cyber risk and recognition of competency gaps are becoming increasingly widespread, particularly among hospitals (91.2% reporting needs in this area). The frequently expressed demand for intensive and widespread training of medical and administrative staff points to a significant deficit in competencies related to incident analysis and response, further exacerbating the sector's vulnerability to cyber threats. It is therefore unsurprising that more than half of healthcare facilities (53%) assess their level of digital maturity as average, while nearly 25% consider it low or very low.

[28] Centre for e-Health (Centrum e-Zdrowia), *VIII Survey on the Level of Digitalisation of Entities Performing Medical Activities*, March 2025, https://cez.gov.pl/pl/page/publikacje [accessed on: 08.02.2026], pp. 5–6; The study covered 11,185 healthcare entities.

In light of the results of the digitalization survey conducted by the Centre for eHealth, the examples of successful cyberattacks on medical facilities in Poland in recent years come as little surprise[29]. Within just eight months of 2025, the healthcare sector recorded the same number of cybersecurity incidents as in the entire year of 2024, namely 946 incidents. The most common attack methods included computer fraud (311 cases), vulnerable services (238 cases, of which as many as 150 were directly related to the exploitation of software vulnerabilities), and ransomware malware (90 cases)[30]. The number of ransomware attacks targeting healthcare facilities has been increasing worldwide at an alarming rate. Over a five-year period, such attacks increased more than sevenfold, from 69 cases reported in 2020 to 506 cases in 2024[31]. This highly unfavorable trend indicates that cybercriminals are increasingly targeting healthcare entities, exploiting both their weaker security posture and their critical societal role. In cases where hospital systems are infected with malware, attackers often remain undetected within the hospital's IT infrastructure for many months, analyzing its architecture, escalating privileges and exfiltrating data. Data indicate that the average time to identify an incident exceeds 270 days, giving attackers over half a year of unrestricted activity[32]. After this period, they reveal their presence by encrypting key systems (such as HIS, LIS, RIS, PACS or patient registration systems), effectively paralyzing the facility's operations[33]. The consequences are severe, particularly for patients, as they lead to the cancellation of surgeries and other planned procedures, necessitate the transfer of patients to other hospitals and, in extreme cases, may pose a real threat to life. From the perspective of medical institutions, such incidents also result in

[29] For example, in March 2025, hackers attacked the Ministry of Interior and Administration hospital in Krakow, paralyzing the hospital's main computer system handling medical records. The attackers encrypted files and demanded a ransom for their decryption, which forced a temporary suspension of admissions and a return to paper records. In April 2025, the entity administering the IKP reported a vulnerability: manual manipulation of the URL in the browser allowed unauthorized access to other patients' medical records. The user who reported the issue managed to access the medical records of four other individuals this way. In November 2023, hackers attacked data stored on ALAB Laboratoria servers using ransomware, which blocked access to the computer system, and then demanded a ransom to restore it to its original state. Cybercriminals seized approximately 200,000 patient records from 2017-2023.

[30] Number of data protection incidents in the healthcare sector: 2021 – 150, 2022 – 251, 2023 – 405, 2024 – 1028, I-VIII 2025 – 946. Centrum eZdrowia, www.cez.gov.pl [accessed on: 30.01.2026].

[31] https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/csirt-cez-ostrzega-wzrasta-liczba-incydentow-cyberbezpieczenstwa-w-ochronie-zdrowia [accessed on: 28.01.2026].

[32] https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025 [accessed on: 07.02.2026].

[33] Healthcare continues to experience the longest detection times across all industries requiring nearly *4*0 additional days beyond the global average. 2025 Data Breach Investigations Report, Healthcare Snapshot,https://www.verizon.com/business/resources/infographics/2025-dbir-healthcare-snapshot.pdf [accessed on: 07.02.2026].

data loss and significant financial damage[34]. A further critical gap remains the lack of business continuity plans and post-incident procedures. Meanwhile, regulations such as the NIS2 Directive explicitly require not only technical safeguards but also prepared scenarios for incident response and system recovery.

Medical data are becoming an increasingly attractive target for cybercriminals also due to their intrinsic value and monetization potential. They are highly valuable on the black market because they contain critical information that can be readily exploited for social engineering, phishing attacks and fraud. Such data may be used for insurance fraud, identity theft, as well as the illicit acquisition of medications through fraudulent prescriptions or abuses related to falsified sick leave certificates, vaccination certificates or other medical documentation.

5. Towards a Systemic Model of Cybersecurity in Public Health: Key Recommendations for Systemic Improvement

In recent years, we have witnessed an unprecedented increase in the volume of data generated and processed in digital form. Data have become one of the key resources of the modern economy, forming the foundation of numerous business models, research and development projects and innovation processes. This trend is particularly evident in the healthcare sector, where medical data are used not only for the ongoing treatment of patients but also for scientific research, the improvement of therapies, the planning of health policies and the deployment of solutions based on artificial intelligence and personalized medicine. The dynamic growth of digital data therefore represents a significant social opportunity, while at the same time generating new and increasingly serious risks. Parallel to technological development and the growing dependence of healthcare systems on ICT infrastructure, the scale of cyberattacks has been increasing, particularly those targeting sensitive data such as health-related information. Medical data belong to the most valuable categories of information on the black market, as they may be used for criminal purposes, blackmail or manipulation. At the same time, medical institutions remain among the least protected entities within the digital ecosystem. This situation results from the accumulation of several structural factors, including chronic underfunding of the healthcare system, limited budgets for IT and cybersecurity investments, shortages of specialized personnel and insufficient level of knowledge and awareness of threats. A particularly important element of this landscape is the human factor. Experience shows that even the most advanced technologies do not provide real security if they are not properly implemented,

[34] The average cost of a data breach in the global healthcare sector is estimated at $7.42 million in 2025,www.cez.gov.pl [accessed on: 08.02.2026].

configured and used. It is the human being who ultimately determines the effectiveness of technical solutions, both at the system design stage and during everyday operation. The lack of clear procedures, insufficient training and the routine neglect of cyber hygiene principles by medical and administrative staff significantly increase the vulnerability of healthcare institutions to incidents. Cybercriminals skillfully exploit these weaknesses, relying not only on technical attack methods but also on social engineering, phishing and manipulation of user behavior.

Awareness of these challenges led in 2025 to an initiative undertaken by the Council for Digitalization operating under the Minister of Digital Affairs[35], aimed at formulating recommendations to improve the level of cybersecurity in the healthcare sector[36]. These recommendations respond to a broader need to enhance coordination of activities, reduce regulatory fragmentation and bridge the gap between growing technological requirements and the actual organizational capabilities of healthcare entities. They demonstrate that improving cybersecurity cannot rely solely on technology but requires coherent regulatory, organizational and educational measures that take into account the specific characteristics of the healthcare sector and its key role in public security. The recommendations of the Council for Digitalization issued in 2025 should be viewed as an attempt to provide a systemic response to the shortcomings of the current cybersecurity regulatory model in the healthcare sector. Their significance lies not so much in introducing entirely new normative solutions, but rather in indicating the necessary directions of change within the framework of existing legal instruments.

The Council for Digitalization clearly points to the need to improve the coordination of cybersecurity activities in the healthcare sector at the central level. The absence of a single authority responsible for defining directions, priorities and standards leads to a dispersion of competences and inconsistency in actions taken. The recommendations move toward a clearer delineation of the roles of individual public institutions and the strengthening of cooperation mechanisms between government administration, healthcare entities and institutions responsible for cybersecurity. To this end, the Council recommended the establishment of a working group tasked with identifying security gaps and vulnerabilities within the healthcare sector and preparing legal, organizational and technical solutions aimed at enhancing the security of patient data.

[35] More information about the Council for Digital Affairs (its composition, tasks and recommendations) can be found at: https://www.gov.pl/web/cyfryzacja/rada-do-spraw-cyfryzacji [accessed on: 08.02.2026].

[36] Council for Digitalisation (Rada do Spraw Cyfryzacji) at the Ministry of Digital Affairs, *Statement of the Council for Digitalisation on Cybersecurity in the Healthcare Sector*, April 2025, https://www.gov.pl/attachment/cd8ef083-f370-49b7-b7c7-b17c97ebd404 [accessed on: 07.02.2026].

Another key postulate concerns the development and implementation of a uniform, mandatory catalogue of minimum cybersecurity requirements applicable to all entities within the healthcare system. The recommendations emphasize that the current freedom in selecting technical and organizational measures leads to significant disparities in security levels. The applied standards should take into account the specific nature of medical data, the role of critical systems and the growing cyber threats, while at the same time remaining feasible for implementation by smaller entities. Consequently, the most urgent actions identified include the immediate definition of minimum requirements for commercial medical practice software applications. Although the Act on the Healthcare Information System imposes on service providers and entities maintaining medical registers an obligation to ensure compliance of their ICT systems with minimum technical and functional requirements[37], service providers tend to focus primarily on functionality while marginalizing technical security aspects. For this reason, the Council recommended imposing a legal obligation to ensure specific minimum cybersecurity requirements for the systems of service providers and entities maintaining medical registers. Such requirements should include, inter alia, mandatory two-factor authentication, enforced use of strong passwords, account lockout after several unsuccessful login attempts, automatic session timeouts, role-based access control, encryption of network traffic, access control mechanisms, logging and monitoring of audit trails and automatic alerts in the event of detected suspicious activity.

An important area of the recommendations concerns the enhancement of digital competencies and awareness of cyber threats among medical staff, administrative personnel and management. In its position, the Council emphasizes that the human factor remains one of the weakest links in the system and that the lack of regular and practical training significantly increases vulnerability to social engineering attacks. The recommendations advocate for systemic, cyclical educational programs tailored to different roles within healthcare organizations. Cybersecurity should be treated as an integral element of risk management in healthcare entities, therefore, beyond a permanent educational component, medical institutions should be required to implement procedures related to business continuity planning, including regular testing of contingency plans. The recommendations stress the need to move away from a reactive approach toward a model based on risk analysis, resilience testing and continuous improvement of procedures. This includes not only prevention but also preparedness for incidents and response procedures in the event of a cybersecurity incident. Furthermore, healthcare sector entities should apply

[37] The Public Information Bulletin of the Minister of Health specifies the technical and functional requirements for service providers and entities maintaining medical records.

basic security measures to the devices and information systems they use, such as regular updating of operating systems.

In conclusion, the recommendations of the Council for Digitalization reveal the need to transition from a fragmented and reactive model of cybersecurity regulation in healthcare to a systemic, integrated and proactive approach. Their implementation requires not so much the multiplication of new obligations as better coordination of existing regulations, clarification of standards and genuine organizational and financial support for healthcare entities. In this sense, they constitute an important starting point for further *de lege ferenda* discussion on the future shape of cybersecurity in public health.

The scale, velocity, and heterogeneity of contemporary data generation underscore an increasingly visible gap between technological capabilities and existing legal and regulatory frameworks. In the absence of coherent, sector-specific and adaptive data governance and cybersecurity standards, the exponential growth of data, particularly sensitive health data, amplifies systemic vulnerabilities within digital public services. This reality calls for a deliberate transition from fragmented and reactive regulatory approaches towards a coordinated, risk-based and forward-looking model of cybersecurity governance in public health. Only such approach can ensure that the benefits of big data and advanced digital technologies are realized without undermining fundamental rights, public trust and the operational resilience of healthcare systems and their underlying digital infrastructures.

References

Sources

Act of 17 February 2005 on Computerisation of Activities of Entities Performing Public Tasks, Journal of Laws 2024, item 307.

Act of 6 November 2008 on Patients' Rights and the Patients' Rights Ombudsman, Journal of Laws 2024, item 581.

Act of 28 April 2011 on the Information System in Healthcare, Journal of Laws 2023, item 2465, as amended.

Act of 5 July 2018 on the National Cybersecurity System, Journal of Laws 2023, item 913, as amended.

Act of 10 May 2018 on the Protection of Personal Data, Journal of Laws 2019, item 1781, as amended.

Centre for e-Health (Centrum e-Zdrowia), *VIII Survey on the Level of Digitalisation of Entities Performing Medical Activities*, March 2025, https://cez.gov.pl/pl/page/publikacje [accessed on: 08.02.2026]. Code of Conduct for the Health Care Sector adopted pursuant to Article 40 of Regulation (EU) 2016/679, applicable to healthcare providers and data processors, 11 December 2023, https://uodo.gov.pl/pl/file/4525 [accessed on: 06.02.2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European strategy for data, COM/2020/66, Brussels, 19.02.2020.

Council for Digitalisation (Rada do Spraw Cyfryzacji) at the Ministry of Digital Affairs, *Statement of the Council for Digitalisation on Cybersecurity in the Healthcare Sector*, April 2025, https://www.gov.pl/ attachment/cd8ef083-f370-49b7-b7c7-b17c97ebd404 [accessed on: 07.02.2026].

Checkpoint Research, Cybersecurity Report 2026, https://www.checkpoint.com/security-report/ [accessed on: 07.02.2026].
CERT Polska – NASK, *Annual Report on the Activities of CERT Polska,* April 2023.
CSIRT NASK (CERT Polska), *Monthly Summary Report No. 4/2025*, December 2025, pp. 5–6.
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152. ENISA – European Union Agency for Cybersecurity, "Cyber Hygiene in the Health Sector", September 2025, https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber %20Hygiene% 20in%20the%20Health%20Sector.pdf [accessed on: 06.02.2026].
European Commission, *Communication from the Commission to the European Parliament and the Council: European Data Union Strategy – Unlocking Data for Artificial Intelligence*, Brussels, 19 November 2025, COM(2025) 835 final, pp. 7–8.
European Commission, Data, https://digital-strategy.ec.europa.eu/en/factpages/data [accessed on: 03.02.2026].
International Data Corporation, https://www.businesswire.com/news/home/2020051300 5075/en/IDCs-Global-StorageSphere-Forecast-Shows-Continued-Strong-Growth-in-the-Worlds-Installed -Base-of-Storage-Capacity [accessed on: 02.02.2026].
Implementing the European Health Data Space across Europe, eitHealth Think Tank, https://eithealth.eu/wp-content/uploads/2024/04/EIT_Health_ThinkTank_Implementing_the _EHDS_across_Europe_23.04.24.pdf., April 2024 [accessed on: 07.02.2026].
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, https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng [accessed on: 07.02.2026].
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, p. 1, as amended. Regulation of the Council of Ministers of 21 May 2024 on the National Interoperability Framework, minimum requirements for public registers and electronic information exchange, and minimum requirements for ICT systems, Journal of Laws 2024, item 773.
Regulation of the Minister of Health of 6 April 2020 on the types, scope and models of medical documentation and the manner of its processing, Journal of Laws 2024, item 798.
Statista Global Data Platform, https://www.statista.com/statistics/871513/worldwide-data-created/ [accessed on: 01.02.2026].
TechSci Research LLC, https://www.techsciresearch.com/report/big-data-in-healthcare-market/4009.html [accessed on: 02.02.2026].
J. Thomason, "Data, Digital Worlds, and the Avatarization of Health Care", *Global Health Journal*, Vol. 8, Issue 1, March 2024, pp. 1–3. https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/csirt-cez-ostrzega-wzrasta-liczba-incydentow-cyberbezpieczenstwa-w-ochronie-zdrowia [accessed on: 28.01.2026].
https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_pl [accessed on: 07.02.2026].
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025 [accessed on: 07.02.2026].
2025 Data Breach Investigations Report, Healthcare Snapshot, https://www.verizon.com/ business/resources/infographics/2025-dbir-healthcare-snapshot.pdf [accessed on: 07.02.2026].

Literature

European Commission, *The Impact of the European Health Data Space Regulation and the Open Data Directive on Citizens*, data.europa.eu, Publications Office of the European Union, July 2025.

Kaźmierczyk P., Lukosek D., Czarnuch M., Horyń A., *Medical Data in Physicians' Practice: Current State and Desired Changes*, Report of the Network of Physician Innovators, Supreme Medical Chamber, 2023.

Ryś A., "European Health Data Space – New Challenges and Opportunities", *Med. Prakt.*, 2025, no. 3, pp. 110–119.