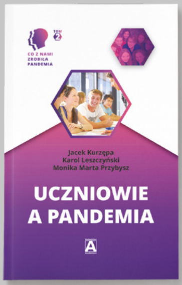
HEALTH SECURITY AND CYBER INNOVATIONS IN HEALTH CARE

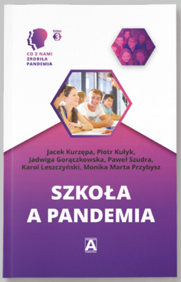
Wydawnictwo
Academicon

Publikuj
z nami
w open
access!

HEALTH SECURITY – POLICY – COMMUNICATION

CO Z NAMI ZROBIŁA PANDEMIA
Jacek Kurzępa
BADANIA IN STATU NASCENDI W CZASIE PANDEMII SARS-COV-2


CO Z NAMI ZROBIŁA PANDEMIA
Jacek Kurzępa
Karol Leszczyński
Monika Marta Przybysz
UCZNIOWIE A PANDEMIA


CO Z NAMI ZROBIŁA PANDEMIA
Jacek Kurzępa, Piotr Kułyk, Jadwiga Gorączkowska, Paweł Szudra, Karol Leszczyński, Monika Marta Przybysz
SZKOŁA A PANDEMIA

HEALTH SECURITY AND CYBER INNOVATIONS IN HEALTH CARE

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

Wydawnictwo
A
Academicon

HEALTH SECURITY AND CYBER INNOVATIONS IN HEALTH CARE

Edited by

Katarzyna Marzęda-Młynarska
Liliana Węgrzyn-Odzioba
Aneta Wójciszyn-Wasil
Justyna Kięczkowska

Lublin 2025

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

Series: Health Security. An interdisciplinary perspective

Reviewers: prof. Henryk Chałupczak, dr Łukasz Potocki

Publishing support:
Studio DTP Academicon | e-mail: dtp@academicon.pl | www: dtp.academicon.pl | managing editor: Monika Pecyna; typeset: Marta Szajdzińska, Karol Cichoń; cover: Patrycja Waleszczak

Translation and proofreading: Wojciech Łysakowski

Publication supported by The Polish Academy of Sciences, Branch in Lublin

ISBN [ebook]: 978-83-67833-25-7

DOI: 10.52097/acapress.9788367833257

Publisher: Academicon Press
ul. H. Modrzejewskiej 13, 20-810 Lublin
tel.: 603 072 530
e-mail: wydawnictwo@academicon.pl
www: omp.academicon.pl

Księgarnia online: ksiegarnia.academicon.pl

SPIS TREŚCI

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

INTRODUCTION

In the face of dynamically developing digitalisation and technological transformation of the modern world, healthcare is facing a number of challenges that are redefining traditional models of medical care, data management and population healthcare. In particular, cyber innovations – including artificial intelligence, analysis of large data sets (big data), the Internet of Things (IoT), blockchain, and telemedicine technologies – are becoming the pillar of modern healthcare systems, transforming the methods of diagnosing, treating and monitoring health. At the same time, advancing digitalisation brings with it challenges related to the security and integrity of medical data, protection of patient privacy, and ensuring the resilience of systems to cyber threats. Therefore, the issue of cyber innovation is becoming crucial for health security at both the individual and societal level.

The Department of International Security of the Institute of International Relations of Maria Curie-Skłodowska University, the Department of International Political Relations of the Institute of International Relations of Maria Curie-Skłodowska University, the Department of Visual Communication and New Media of the Institute of Journalism and Management of the Catholic University of Lublin, the XVI Commission of Political Science and International Relations of the Branch of the Polish Academy of Sciences in Lublin and the Foundation for International Research have cooperated for the fourth time to organize the 4th National Scientific Conference on Health Security and Cyberinnovations in Healthcare.

The 4th National Conference is a series of annual meetings on the issue of broadly understood health security and the analysis of factors that have a direct impact on them. The main goal of the conference is to combine practice and theory during conference panels and workshops of key importance for broadly understood health security. The event is also an excellent opportunity to establish cooperation with entities directly responsible for the health care system, health policy, and to learn about solutions in the field of health care. It is also a platform for the exchange of information and experiences related to the challenges for health security in Poland, Europe and the world, serving to integrate the community of practitioners and specialists in the field of politics, medicine and communication. The initiative is a platform for the exchange of information and experiences related to the challenges for health security in Poland, Europe and the world, serving to integrate the community of practitioners and specialists in the field of politics, medicine and communication.

The aim of the 4th Conference was a broad discussion on the impact of cyber innovations on the health security of the state and citizens. The organizers proposed a discussion in the following thematic areas:

1. Healthcare Policy and Cyber Solutions: Building a Secure and Resilient Infrastructure;
2. Medicine, Health Security and Cyber Development: Challenges and Opportunities in the Digital Age;
3. Cyber Development in Medicine: Transforming Communication and Healthcare.

The selection of thematic scope resulted from the definition of the fundamental role of cyber innovations in modern medicine and the healthcare system. The issues raised were also intended to highlight the opportunities that cyber progress brings and to prepare for the challenges related to their implementation.

The cooperation in organizing this scientific event, the UMCS, KUL, the Polish Academy of Sciences and the Foundation for International Research presenting various fields and research tools allowed to show integrated and multidimensional actions to ensure health safety in the face of technological progress. It is also an example of a new mechanism of action of Lublin universities, undertaking cooperation with other entities in order to exchange experiences and information.

The article by Marek Pietraś, *Specificity of securitisation of health security risks*, includes the assumption made by the Author that health security is a dimension of security, a result of securitization of its threats. He classifies it as a second-generation dimension of security, conditioned more by the processes of globalization and global mobility. The Author also concludes that health security is a result of securitization of threats made by political entities formulating a speech act and at the same time playing the role of public opinion, accepting the speech act.

In the article by Małgorzata Gruchoła, *Ethical challenges related to the use of medical artificial intelligence in the healthcare system*, the author indicates the criteria for the ethicality of AI in medicine and healthcare, and also presents the risks associated with the use of medical artificial intelligence and solutions that can eliminate them.

Katarzyna Marzęda-Młynarska in the article *Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience* shows the impact of the COVID-19 pandemic on international food systems. The author also analyses the challenges and prospects for international food systems in the context of the experience of the COVID-19 pandemic, including the impact on food security, resilience to unpredictable phenomena and technological innovation.

Study, conducted by Justyna Szulich-Kałuża, Małgorzata Sławek-Czochra in their text entitled *COVID passports in Poland and Europe – symptom ofpost-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis* was created on the basis of empirical research and discourse analysis, examines whether Covid passports were perceived by citizens of Poland and other European Union countries as an effective tool leading to post-pandemic normalization or as a behavioral intervention aimed at changing citizens' behaviour.

Tomasz Bichta in the article *Angola's health security system* presents the health care system in Angola. Both in legal and institutional terms. The author presents the actual state of affairs in the field of health security of citizens, drawing attention to numerous problems, but also attempts to overcome them.

Justyna Kięczkowska and Liliana Węgrzyn-Odzioba in the article *Online consultation – opportunity or threat to health security?* analyze the challenges and threats related to this type of services and present best practices and recommendations aimed at minimizing the risk. In the second text Security of medical data

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

in Poland after the Covid-19 pandemic, the authors analyse the course of the digitization process in the area of medical data security understood as "health data" and "personal data" of patients.

Justyna Kięczkowska and Liliana Węgrzyn-Odzioba in the article *Security of medical data in Poland after the Covid-19 pandemic* describes the evolution of the medical data security strategy in Poland after the COVID-19 pandemic, to identify the main challenges and to discuss innovative approaches and technologies for the protection of patient data. The analysis will cover both changes in legal regulations and practical solutions used by medical facilities to ensure data security.

Stanisław Bichta in the article *E-public relations in healthcare and associated risks* describes conducting public relations activities in the healthcare system. He presents threats and opportunities for healthcare system entities related to their presence on the Internet.

Paulina Szaniawska in her article *Ethics and security related to AI in medicine* discusses issues related to transparency, inequalities in access to AI, and the impact of these technologies on the doctor-patient relationship. She devotes particular attention to legal regulations that should keep up with the rapid pace of AI implementation in medicine.

Aleksandra Kramek in her article *AI in Modern Medicine* analyses the most important applications of AI in various fields of medicine, such as support in mental health treatment, telemedicine and care for chronically ill patients. She also addresses ethical issues and challenges related to the implementation of AI in medicine, including patient data protection and transparency of system operation.

Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025).
Health security and cyber innovations in health care. Wydawnictwo Academicon.
https://doi.org/10.52097/acapress.9788367833257

Marek Pietraś

Faculty of Political Science and Journalism of the Maria Curie-Skłodowska University,
Institute of International Relations UMCS
E-mail: marek.pietras@mail.umcs.pl
ORCID: 0000-0002-9334-7737

SPECIFICITY OF SECURITISATION OF HEALTH SECURITY RISKS

Abstract: Health security is a dimension of security, a consequence of the securitisation of its threats. It is proposed to be included in the second generation of security dimensions, conditioned more by the processes of globalisation and global mobility. The first generation includes the dimensions proposed by the Copenhagen School, conditioned primarily by the end of the Cold War. The assumption was made that health security is the result of the securitisation of its threats by policy actors formulating the speech act and, at the same time, playing the role of public opinion, accepting the speech act. In view of this, the assumption was formulated that the securitisation of security threats by policy actors, with the limited presence of academia, is specific to second-generation security dimensions. The aim of the article is to identify the specificities, unique features, of the securitisation of health risks. The focus is on: firstly, reconstructing the assumptions of the concept of securitisation as a research tool, the importance of the speech act, the role of public opinion with emphasis on the positional power of the subject formulating the speech act. Secondly, the object of securitisation was analysed in the form of health threats, identifying their scope, but also emphasising that these threats, while being destructive directly to human health and life, are also destructive to social systems, but are also conditioned by the quality of these systems such as globalisation processes. Thirdly, the process of securitisation of health threats by policy actors, mainly the United States, was the subject of analysis.

Keywords: health security, health security threats, securitisation, positional power, Covid-19.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

INTRODUCTION

Health security is another, one of the latest securitised, non--military dimensions of national or international security (Pietraś, 2022, pp. 15–50). It confirms that security, while being one of the most important values in the life of society, is at the same time a dynamic process of broadening and deepening its material scope by further dimensions or sectors and its subjective scope, going beyond the earlier state-centric understanding. This means that the dynamics and variability of the subject and object scopes of security is a dependent variable, conditioned by an independent variable in the form of changing social reality, the dynamics of intra-state and international social life. This is an important methodological assumption of this article, as is the analytical application of the concept of securitisation proposed by the Copenhagen School (Waever, 1995, pp. 46–86; 2004, pp. 17–20; Taureck, 2006, pp. 53–61; Buzan *et al.*, 1998, pp. 32–36).

In the 21st century, under the conditions of the end of the Cold War and globalisation processes, health threats – along with terrorism and cyber threats – have shown the greatest dynamics of growth. This is confirmed, for example, by the Covid-19 pandemic of global scope, preceded by numerous epidemics in various regions of the globe. This is a time of relative growth in the importance of health threats, also known as the microbiological turn in security studies. It should therefore come as no surprise that these threats have been securitised, becoming another dimension of broad (*comprehensive*) security, contributing to its progressive complexity.

In view of the above, it is assumed that each dimension or security sector is distinguished by its own specific characteristics. In other words, each dimension is specific, acquiring distinct, autonomous characteristics that distinguish it from other dimensions. It is proposed that the health dimension be counted among the second generation of security dimensions (Pietraś, 2023, p. 7) conditioned primarily by the processes of globalisation and the new quality of social life inherent in them. It is proposed that the five dimensions of security identified by the Copenhagen School (Bu zan *et al.*, 1998, pp. 32–36), dimensions conditioned primarily by the end of the Cold War, be counted in the first generation.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

In the context of the assumption of autonomy, the specific characteristics of the different dimensions of security, the aim of this article is to analyse the distinctiveness, the specificity of the securitisation of the health dimension, i.e. the integration of security into the field of security studies and practice. In order to realise this objective, the subject of analysis will be: 1) the essence of securitisation; 2) the specificity of the object of securitisation, which are health security threats; 3) the specificity of the process of securitisation of these threats; 4) the specificity of the notion of "health security", which is the result of the securitisation process.

THE ESSENCE OF SECURITISATION

Health problems were included in the analysis of security studies, securitised, after the end of the Cold War, in a radically changing international environment and accompanying change in the understanding of security. During the Cold War, health threats were categorised as *'low politics'* (Fidler, 2005, p. 180; Farrell, 2018, p. 554), recognising that they were humanitarian rather than political problems (Youde, 2018, pp. 535–536). Probably for the first time in the documents of international organisations, the term *'health* security' appeared in the report of the United Nations Development Programme (UNDP) published in 1994. It was used in connection with the proposal of the concept of *human security*, considering it as one of its 7 components (UNDP, 1994, pp. 24–26).

To explain the change in attitudes towards health risks and their securitisation, two factors appear to be relevant. Firstly, a change in social reality. Coupled with a general trend towards an increase in the importance of non-military dimensions of security, the variety, intensity and number of victims of human health threats has increased as a result, above all, of the increasing number of epidemics. Secondly, philosophical inspiration and associated with it a kind of acquiescent intellectual climate in the form of the biopolitisation of security and politics (Dillon, 2008, pp. 265–266, 269). This implies a kind of synergy of factors relevant to and for the earlier identification of

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

non-military dimensions of security in the form of changing realities, resulting new threats and intellectual acceptance.

The aforementioned factors created the rationale for, but did not determine, the integration of health threats into security thinking and practice. This happened as a result of the securitisation of these problems, i.e. the recognition of them as existential threats to national and international security. Securitisation, following the intellectual legacy of the 1960s (Austin, 1969), was proposed and popularised by the Copenhagen School of Security Studies in the late 1980s and early 1990s (Buzan *et al*., 1998, pp. 32–36; Waever, 1995, pp. 46–86). It provides a theoretical framework for integrating threats into the field of security analysis and political responses to them, being a discussion-provoking concept for changing security thinking (Stritzel, 2007, p. 357; Yuk-pink Lo & Thomas, 2018, p. 568; Taureck, 2006, p. 55). By proposing the concept of securitisation, the Copenhagen School has made an important contribution to redefining security, broadening its material scope by including further non-military dimensions (Ziętek, 2017, pp. 23–42) including health security.

An analysis of the specificity of health security securitisation requires a reconstruction of the assumptions of the Copenhagen School understood as a research tool. Ole Waever and Barry Buzan defined securitisation as an effective speech act (*speach act*) through which a specific social phenomenon, e.g. a public health threat, is intersubjectively treated by a specific subject as an existential threat to a designated object of reference, e.g. the state, in order to justify the application of extraordinary measures to counter this threat (Buzan & Waever, 2003, p. 491). What is important is therefore the subjective feeling (Williams, 2011, pp. 454), and through it and its verbalisation the social construction of the dimensions of security, without them being determined solely by material conditions (Balzacq & Guzzini, 2015, p. 99).

The securitisation process combines three elements: 1) speech acts, utterances, declaring the referenced phenomenon, the process of action, to be an existential threat; 2) the securitising subject, formulating the speech act; 3) the public, the audience, who accept or reject the content of the speech act. According to the Copenhagen School, the securitising subject is the one who, by formulating the speech act, declares that someone or something, being the object of reference, is existentially threatened. A feature of securitisation processes is the variety of actors involved. It can be the state, an international institution, an NGO, academic institutions, individuals, etc. The object of reference, in turn, can be mainly entities that are perceived as existentially threatened, having a right to survival (Buzan *et al.*, 1998, pp. 36–40). The object of reference and the existential threats to it are diverse and depend on the dimension or sector of security. It can be the state, its sovereignty, but also the national economy, national identity, the state of the environment, but also the state of the health of society with possible consequences for other sectors (Emmers, 2008, p. 110).

The dynamics of the securitisation process consist of two stages. The first is the speech act, the discursive presentation of a particular phenomenon, entity, etc. as an existential threat to the object of reference. It has even been formulated in this context that security is seen as something that is created by language (Hansen, 1997, p. 381), and therefore a speech act. This is half-hearted and simplistic thinking, as 'language' merely verbalises an emotion, a fear of a particular phenomenon, an action perceived as a threat. It is therefore more reasonable to say that security is created by emotions verbalised by a speech act. India Wright has even formulated the view that security is a discursive practice (Wright, 2021), but conditioned by emotions. It has also been noted in the literature that the language of security and health discourse contains common concepts like defence, containment, elimination, front line. Infectious diseases can be an instrument of warfare (Howell, 2014, p. 977).

Using the language of security does not mean that a defined threat must automatically become part of security thinking and provision. Stage two occurs when the subject of securitisation is effective in convincing the audience, i.e. the public, politicians, international officials, and others, that the object of reference is existentially threatened. This means that the Copenhagen School sees security, its threats, as socially constructed through securitisation (McDonald, 2008, p. 563). Existential threats are intersubjectively recognised as such by the subject securitising them, but also by the public to whom the speech act is addressed. Consequently, each act of securitisation reflects

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

a social or political preference and is a type of decision most often with serious consequences for political practice (McDonald, 2008, p. 112–114).

An important element in the analysis of securitisation processes – also in relation to health security – is the actor initiating the speech act. Representatives of the Copenhagen School suggest paying attention to who is privileged in the formulation of the speech act, i.e. the articulation of a sense of existential threat. They emphasise the need to take into account the securitisation of the behaviour of the centres of political power in the analysis, considering them as having priority in the formulation of the speech act. For this reason, they treat the area of security as 'structured' in that certain actors such as the state apparatus are particularly privileged in the formulation of the speech act, the articulation of speech (Buzan *et al.*, 1998, pp. 31–32).

A valuable proposal, which is a modification of the assumptions of the Copenhagen School, was proposed by Holger Stritzel. He considered securitisation to be a three-layered process involving text, context and the positional power of the subject formulating the speech act. The socio-linguistic context is important, i.e. the narrative accompanying the verbalisation of an existential threat, the content of the speech, the concepts used, but also the historical moment, the context of the situation, thinking in terms of an idea whose time has come in the sense of reflecting social or political expectations. These are essential elements for understanding the speech act, the message addressed to the public. The positional power of the subject of securitisation, on the other hand, is conditioned by the socio-political context of its functioning, prestige, authority, position in the hierarchy of social life (Balzacq, 2005, pp. 180–181). This context is important for the effectiveness of securitisation, for the potential for influence of the securitising subject and the construction of the speech act, but also for its reception by the public (Stritzel, 2007, pp. 364–370). Thinking in terms of positional power is crucial for analysing the specificity of the securitisation process of health security threats. This is discussed later in the article.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

SPECIFICITY OF THE SUBJECT OF SECURITISATION, I.E. HEALTH SECURITY RISKS

An important element of the analysis of securitisation is to identify its object, i.e. to answer the question what is or has been securitised? Answering this question involves identifying the risks specific to each security dimension. F. X. Kaufman defined them as the possibility of one of the negatively valued phenomena occurring (Kaufman, 1970, p. 167). This means that they do not have to be identified exclusively with an enemy acting intentionally, creating existential threats, but also with phenomena, processes that are not necessarily intentional, that can cause an existential effect or such subjective perception of them. In order to identify the specificity of securitised health threats, it is proposed to focus on three elements: 1) the health risks that directly affect people's health and lives, 2) the impact of these risks on social life with the potential to destabilise it, 3) the determinants, the context of social life that favours health risks.

With regard to health threats directly affecting human health and life, it should be emphasised that their feature is their complexity and "hybrid nature". They combine non-intentional processes, phenomena with the possibility of intentional, hostile application, and to this is added the diversity of threats, their wide range of subject matter. These include, first and foremost, as if by way of a matter of course, infectious diseases taking the form of epidemics or pandemics and, in their context, the problem of crossing the species barrier, the phenomenon of bioinvasion, the problem of increasing resistance to antibiotics, as well as bioterrorism and the possibility of using biological weapons.

Infectious diseases are a particular threat to health security. The HIV/AIDS epidemic set in motion the securitisation of health threats, and the Ebola epidemic reinforced this process. Epidemics with even global proportions of their victims occurred in the 20th century, already overloading the health systems of many countries (Rockenschaub *et al.*, 2007, p. 20). Since the beginning of the 21st century, the diversity and intensity of epidemics has clearly increased, reflecting several trends. Firstly, new pathogens such as Nipah virus, Marburg, Ebola,

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

MERS-Cov. virus, coronavirus, SARS, A/H5N1 influenza, but also A/H1N1, A/H7N9, A/H5N6 in different parts of the globe have emerged (Gostin *et al.*, 2017, p. 53). Secondly, there were recurrences of previously known infectious diseases like cholera, tuberculosis, influenza, measles, meningitis, yellow fever. Thirdly, there has been an intentional use of anthrax bacteria (Rockenschaub *et al.*, 2007, p. 16).

One example of the potential for threats to national and international security caused by epidemics is the Ebola virus and the Covid-19 pandemic. The Ebola virus was identified in Africa in the mid-1970s. The Ebola outbreak that broke out in Guinea in March 2014 had significant international consequences. It spread to other West African countries such as Sierra Leone, Liberia, Nigeria, Mali, Senegal, and outside Africa it reached Spain, Liberia, the UK and the US. The number of infections is calculated at 28616 and the death toll at 11310. This epidemic has caused: 1) threats to the national security of these countries; 2) the potential to destabilise the region; 3) threats to international security on a global scale (Ifediora *et al.*, 2017, p. 226). In comparison, the number of cases of Pandemic Covid-19 as of mid-April 2024 is 704753890 cases and 7010681 fatalities (Worldometer, 2024).

The spectacularity of infectious diseases, borne out by the Covid-19 experience, the global nature of this pandemic, the variety of impacts and the global media portrayal cannot overshadow the threats posed by non-communicable diseases. In a report for *the World Economic Forum* published in 2011 on the burden of these diseases on the world economy. It projected a reduction in global GDP of up to $46.7 trillion between 30 February 2010 (Bloom *et al.*, 2011).

Crossing the species barrier is becoming a significant threat to health security. Consequently, the interdependence between human, animal and environmental health is increasing. However, the problem is the limited level of knowledge about the relationship between these elements. In addition, the processes of globalisation, increased human and animal mobility are increasing the vulnerability and susceptibility in the relationships between humans, animals, the population and the environment. As a result, the risk of epidemics is increasing (Bouskill *et al.*, 2019, p. 2).

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Another threat is invasive alien species previously in a particular environment. Their spread is called bioinvasion and is the result of the deliberate introduction of some species by humans in order to control others. Applied as early as the first half of the 20th century, it was regarded as a biological problem. Over time, it came to be seen as an economic problem, linked to globalisation processes and a security problem. In an environment of globalisation processes, there is a concern that these microbes can spread globally, and hence are called pathogens of globalisation (Bright, 1999, pp. 51–64). Hence, an important problem related to bioinvasion is included in the question of risks to human health. These pathogens are also a significant problem for food security and a growing problem for the national security of states. The opinion is being formulated that they pose a threat to the strength of a state, undermining its economic potential and the health of its population, i.e. its demographic potential, and consequently bring an element of biosecurity into thinking about state security (Stoett, 2010, pp. 103–110).

Antibiotic resistance is also considered a threat to health security. Antibiotic-resistant infectious diseases emerging in one country mean a threat to health and economic processes in other countries. It is estimated that in the second decade of the 21st century, drug-resistant pathogens were responsible for the deaths of approximately 700,000 people each year. G8 health ministers in 2013 identified antibiotic resistance as a major health security challenge for the 21st century. This threat is distinguished by several specific features. Firstly, there is no country of origin with which this threat can be identified. Second, antibiotic resistance arises in multiple ways and simultaneously among humans and animals. Third, the linking of this resistance to the food chain implies the need for complex solutions that address different areas of society, rather than simple ones) (Yuk-pink Lo *et al.*, 2018, pp. 570–571, 574).

Health security threats also include bioterrorism, meaning the intentional use of biological agents, such as bacteria, to cause casualties, intimidation and trigger expected behaviour. In the late 20th and early 21st century, several such cases were recorded in the United States. After the terrorist attacks of 11 September 2001, cases of letters containing anthrax bacteria were recorded in New Jersey. Five people died and 17 became ill. Panic was caused among civilians, and several contaminated facilities including Supreme Court buildings and post offices were closed, disorganising community life.

When identifying threats that directly negatively affect people's health and lives, it is important to bear in mind their potential to affect social life with the possibility of destabilising it. This means that they can act as an independent variable with destructive potential, exposing the vulnerability and susceptibility of the organisation and functioning of social life in individual countries, but also regions and even on a global scale. The opinion is even being formulated that pandemics can cause destruction of social life, economic activity comparable to wars, natural disasters or financial crises. This in turn reinforces the argument that these threats, not only because of their health costs, but also because of their economic and political costs, should be treated as a security problem and not as a simple health phenomenon (Gostin *et al.*, 2017, p. 57).

In assessing the social impact of the Covid-19 pandemic, attention has been paid to the destabilising effects at the level of states and to the effects at the level of the international system. With regard to the state level, the vast majority of states under Covid-19 saw restrictions on civil liberties and the introduction of repressive law enforcement measures. There were social protests in many African states. The social and economic impacts were particularly felt in many countries of the Global South, reflecting the asymmetry of vulnerability and resilience of many of these countries to epidemics under lower levels of development. In sub-Saharan African countries, 13.5 million jobs were lost during the Covid-19 pandemic between 2020 and 2021, and 5 million people were placed in extreme poverty (Paul, 2024). And in Africa, the pandemic hit young people hard, limiting access to education and making it difficult to access education.

At the level of the international system, the Covid-19 pandemic was the cause of the global recession, the downgrading of the GDP of many countries, and had geopolitical effects, contributing to the deterioration of relations between the great powers amid a reduction in economic ties between them, especially between the United States and China. Economic ties weakened

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

and nationalisms in the Eurozone were unleashed. The pandemic became a factor in accelerating the geopolitical changes taking place at the level of the global international system. It contributed to increased instability, disrupted supply chains, reduced food supplies and rising inflation. Food insecurity and political instability and conflict were feared (Nkang *et al.*, 2022, p. 37).

In the context of the negative effects on social life of health security threats, the opinion is even being formulated that pandemics can cause its destruction comparable to wars, natural disasters or financial crises. This in turn reinforces the argument that these threats, not only because of their health costs, but also because of their economic and political costs, should be treated as a security problem and not as a simple health phenomenon (Gostin *et al.*, 2017, p. 57).

An analysis of the specificity of health security threats, of what is being securitised, requires consideration of the social context that favours epidemics or any of the other threats mentioned earlier. Enabling factors operate both at the level of the interior of states and at the level of the international system. At the level of the interiors of states, socio-economic conditions such as poverty, unemployment, migration, difficult housing conditions, limited access to health systems, social exclusion and armed conflict are relevant. Urbanisation processes, large urban centres, *megacities* with the concentration of millions of people in a small space, are important for the spread of epidemics.

Important determinants of the acceleration of the spread of epidemics and the rise of health threats operate at the level of the international system. The increased global mobility of people has made the world more vulnerable and susceptible to infectious diseases that are increasingly difficult to contain within national borders. Former UN Secretary-General Kofi Annan called epidemics ‘problems without a passport’ that require a collective global response. Part of the problem of global human mobility is migration. However, it is important to remember that global human mobility is facilitated by the environment of globalisation processes. This is because of the squeezing of time and space that is characteristic of them, reducing the importance of the previously inhibiting mobility barriers of space, distance and time required to overcome them. Globalisation processes have

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

also contributed to the formation of a culture of consumption and unhealthy lifestyles (Jenkins *et al.*, 2016, p. 334).

SPECIFICITY OF THE PROCESS OF SECURITISATION OF HEALTH SECURITY RISKS

The process of securitisation, according to the Copenhagen School, involves the act of utterance, the verbalisation of emotions related to the perception of an action or phenomenon as an existential threat, and the acceptance of this utterance by the so-called audience to which it was addressed. These elements will be the subject of an analysis of the process of securitisation of health security threats, taking into account its specificity. It has been assumed that besides the content of the speech act, i.e. the object of securitisation, the specific element of this process is the subject formulating the speech act. In the case of the securitisation of health risks, the involvement of policy actors in this process is specific. The analysis will also take into account the distinctiveness of Covid-19 securitisation, especially the rhetoric of the speech act of politicians. The reaction of 'public opinion' to the securitisation of health risks also needs to be analysed.

The presence of policy actors in the formulation of the speech act in the securitisation of health risks seems to be a role reversal compared to the securitisation of security dimensions proposed by the Copenhagen School and with the suggestion of being included in the first, post-Cold War generation of security dimensions (Pietraś, 1997). At that time, the speech act was uttered by academics, with politicians acting as the accepting audience. As early as 1977, Lester Brown of the *Worldwatch Institute* called for a redefinition of national security and the inclusion of economic, energy, environmental and food depletion threats in its understanding (Brown, 1977). Jessica Mathew-Tuchman in 1989 suggested broadening national security to include economic, ecological and demographic dimensions (Mathews-Tuchman, 1989, p. 162). These suggestions were accepted by politicians acting as an 'audience'. They were reflected – i.e. they were securitised – in UN General Assembly resolutions, in the 1991 NATO security strategy, in the early 1990s in CSCE

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

documents and in the security strategies of many countries, including Poland's 1992 security strategy.

What is surprising is the absence significant limitation of the scientific community, its proper epistemic communities in the securitisation of health threats and the assumption of the role of formulating the speech act by politicians, who address the securitisation mainly to other politicians and the public opinion of their own countries, but also of the global one. In view of this, in relation to further dimensions of security, beyond those proposed by the Copenhagen School and conditioned more by globalisation processes than by the end of the Cold War and proposed to be called second-generation dimensions, is political will crucial? Does the involvement of the political actor in the securitisation of health threats, by bringing political pragmatism to the process, confirm the general trend of the increasing importance of political actors, their interests, their need to influence public opinion, in the formulation of the 'speech act' for further non-military dimensions of security?

In relation to a policy actor formulating a speech act that recognises a particular phenomenon as an existential threat, the thinking proposed by Holger Stritzel in terms of the actor's positional power is relevant. This thinking is relevant to answering the question who initiated the securitisation of health threats? In answering this question, it should be recalled that the concept appeared in a United Nations Development Programme (UNDP) report published in 1994, but in the context of the category of *human security* and not on its own. It also does not appear that the UNDP had, at that time and in the then state of low health risks of pandemics, sufficient political positional power to securitise these threats.

To answer the question of the speech act formulator with the intention of securitising health threats, it is important to analyse the relationship between these threats and the foreign policy interests of the United States as the hegemon of the international system at the time and the speech act formulator. As early as the late 1990s, the country recognised that health and threats to it were a legitimate foreign policy and national security concern (Katz, 2007, p. 233). The US National Security Council in 1999 for the first time recognised the health problem of HIV/AIDS as

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

a national security threat. It decided to include the problem of the cross-border spread of infectious diseases and the protection of poor people living in failing states in the scope of US foreign policy (Aldis, 2008, p. 372). The US National Intelligence Council in early 2000 assessed that infectious diseases were complicating US and global security, causing threats to US citizens, its armed forces and destabilising the international environment. It recognised that the importance of infectious diseases as a national security threat had increased (Gannon, 2000). In 2001. Secretary of State Colin Powell recognised that the HIV/AIDS epidemic in Africa was a national security issue (Peterson, 2002, p. 44). The speech acts of US institutions and politicians in favour of securitising infectious diseases are unequivocal (see: Pietraś, 2022, p. 22 *et seq*).

The rationale for such thinking by politicians in the United States, but also in many other Western countries, has created fears among the populations of these countries conditioned by media messages. They activated social pressure on the centres of political power. This in turn conditioned the rationality of politicians and also their decisions at the level of the international system, including their actions in the forum of international organisations. It was in the context of such rationality and preferences of societies and politicians of Western countries that the agenda of international organisations in security matters began to be shaped (McInnes, 2008, p. 284). An explanation for this has also been sought in the views of Michel Foucault and the post-structuralists who believe that the discussion of health security is reflexive thinking about the power structures and interests of highly developed states seeking to protect their populations from emerging diseases in developing states (Kamradt-Scott, 2018, p. 509). The latter, on the other hand, focus on health security primarily from the perspective of development processes and the need to build national health capacities.

The US foreign and national security policy preference for health security, shaped under these conditions, began to be reflected in its actions at the level of the international system, especially at the UN and Security Council, in a situation of the country's hegemonic position. The US ambassador to the UN from 1999 to 2001 argued to UN Secretary-General Kofi Annan, who resisted this argument, that HIV/AIDS – by taking a significant part of a country's population and destabilising its social life – was not a humanitarian problem but a security problem (Youde, 2018, p. 537). In 2000, Vice President Al Gore, in a speech at the UN Security Council, advocated an understanding of security that included infectious diseases (Peterson, 2002, p. 43). This meant that the United States stopped treating public health threats caused by epidemics as humanitarian problems, treating them as national and international security problems. With the exception of Donald Trump's presidency, they have acted as a leader in global health efforts.

Under the conditions of unquestionable 'positional power' resulting from being the hegemon of the international order at the dawn of the 21st century, the national perception of health threats as a security problem, especially threats caused by epidemics, the United States began to transfer to the decisions and actions of international institutions, especially the UN, including the Security Council. Taking advantage of the latter's 'institutional position', they reinforced the speech act and process of securitisation of health threats and, more specifically, the HIV/AIDS epidemic. For this process, 10 January 2000 was a historic moment. It was the first meeting of the Security Council in the new millennium, in the 21st century, and the first in the history of the UN after more than 4,000 meetings, when a health problem was discussed as a security problem in the context of the HIV/AIDS epidemic. It was felt that there was no greater threat at the time than the HIV/AIDS epidemic being both a development and security crisis (Security Council, 2000). As a result of the discussion, on 17 July 2000. The Security Council passed Resolution 1308, which recognised HIV/AIDS as a threat with the potential to have a devastating impact on national and international security (Resolution 1308, 2000). Once again, poverty, infectious diseases with HIV/AIDS and environmental degradation were recognised as threats to international security in a UN General Assembly resolution passed on 2 December 2004 (United Nations, 2004).

It should be emphasised that the securitisation of health threats by the UN, including the Security Council, under conditions of US 'positional power' at the beginning of the 21st century, was carried out primarily in relation to such a threat as the

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

HIV/AIDS epidemic, i.e. an infectious disease with the potential for cross-border spread. It does not seem surprising, therefore, that health care issues came up at the Security Council in the context of subsequent epidemics. In 2014, the Ebola virus outbreak in Liberia, Guinea, Sierra Leone and Nigeria. Resolution 2177 identified this epidemic as a threat to international peace and security, highlighting its potential to destabilise the situation in the affected region, cause social tensions and reduce security (Resolution 2177, 2014).

The securitisation of Covid-19, compared to the securitisation of HIV/AIDS or Ebola, proceeded in a specific way. Firstly, after the experience of previous epidemics, the speech act was formulated tardily by policy actors and, once formulated, the rhetoric of verbalising this threat was distinguished by its sharpness. Second, once formulated, the language of politicians was dominated by the rhetoric of war.

After the experience of the ambiguity of the response to the Ebola virus, the slowness and restraint of the UN Security Council's response to the Covid-19 outbreak is surprising. The subject was not addressed by the body until July 2020. Earlier, on 3 April 2020. The UN General Assembly adopted a resolution identifying the Covid-19 pandemic as a global problem requiring global cooperation (United Nations, 2020). The Security Council on 1 July 2020 passed resolution 2532, which stressed that the unprecedented scope of the Covid-19 pandemic could threaten the maintenance of international peace and security. It also demanded the cessation of existing armed conflicts in order to create the conditions for cooperation to counter the pandemic (Resolution 2532, 2020). The surprising, although explainable political positioning of China as the site of the pandemic's emergence in Wuhan, the failure to clearly identify the Covid-19 pandemic as a threat to international security and the tardiness of the response to this threat, has been criticised by analysts (Charbonneau, 2021, pp. 6–16). What role did China, as a permanent member of the Security Council, play in the context of the tardy response? The occasion set in motion a discussion on the Security Council's powers over non-military security threats (Pobjie, 2020).

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

However, once the speech act was formulated, recognising Covid-19 as a security threat, statements by politicians of individual countries, but also by officials of international institutions, were dominated by the rhetoric of war. President Donald Trump considered the coronavirus outbreak more destructive than the attack on Pearl Harbour, the attack on the World Trade Center, and there was no more destructive attack in US history (BBC, 2020). China's President Xi Jinping summoned the country's citizens to a decisive battle in the war against the Covid-19 pandemic (Lun Tian, 2020). In France, President Manuel Macron acknowledged that the country was at war with the coronavirus (Erlanger, 2020). Italy's Prime Minister at the time, Giuseppe Conte, exhorted Italians to stay at home as the country undergoes its most important test since the end of World War II (Lowen, 2020).

Similar views were formulated by officials of the UN system. The organisation's Secretary-General Antonio Guterres said that in the context of the Covid-19 pandemic, the UN was undergoing its toughest test since its inception in 1945. The pandemic has created a significant threat to peace and security. For this reason, political leaders should pool resources for a generational fight (Guterres, 2020). In turn, WHO Secretary-General Tedros Adhanom Ghebreyesus called the Covid-19 pandemic an enemy of humanity. Seeking to reflect the destructiveness of the pandemic, he compared it to war.[1]

Supported by the United States with the involvement of the UN Security Council, the securitisation of health threats, a 'speech act' formulated by these actors, has met with acceptance from the international community, mainly in the form of decisions by international organisations. In 2004, the UN Secretary-General's report *A more secure world: Our Shared Responsibility,* using the category of 'threats without borders' and referring mainly to the example of HIV/AIDS, highlighted the links between health and security (United Nations *et al.*, 2004, p. 12). WHO has made the health security debate a priority in its

[1] Remarks to the Security Council on the COVID-19 Pandemic,https://www.un.org/sg/en/content/sg/speeches/2020–04–09/remarks-security-council-covid-19-pandemic, accessed 3 August 2024.

2006–2015 programme (WHO, 2006). ASEAN, as a regional organisation, securitised health issues during the SARS epidemic in 2003 (Caballero-Anthony, 2018, p. 602). NATO's 2010 Security Strategy identified 'health risks', identifying threats at the international system level (BBN, 2010). References to health security were not found in the 2003 and 2016 European Union security strategies. The issue of health security using this category appeared in the European Commission's communication of 11 November 2020, i.e. during the Covid-19 pandemic, on the European Health Union and enhancing EU resilience to cross-border health threats (EU Monitor, 2020).

The concept of health security is gaining increasing public acceptance. Under the conditions of the Covid-19 pandemic, the links between the spread of the virus and threats to national and international security were not questioned. However, in the earlier stages of the securitisation of health threats, the involvement of the United States in these activities with its political motivation, there was opposition from some countries in the Global South to the notion of 'health security' and the equating of health and security activities, or justifying to the latter the need for global cooperation in health matters (Aldis, 2008, p. 370). The reasons for the opposition were varied. On the one hand, there was the lack of a universally accepted definition of health security, but especially the differences in its definition between countries in the West and the Global South. On the other hand, many countries of the Global South interpreted thinking in terms of health security as an expression of a partisan definition of interests by Western countries seeking to protect themselves from diseases, epidemics emerging in countries of the Global South and having the capacity to spread across borders (Kamradt-Scott, 2018, p. 501). It has been argued that global health issues only become a priority when developed Western states are threatened. In the case of the Ebola epidemic, media coverage of the epidemic turned it from a problem affecting African states into a problem for Western states, their societies and their security (Roemer-Mahler *et al.*, 2016, p. 376).

Particularly opposed by countries of the Global South, especially Brazil, India, Indonesia, Thailand, was the proposal and attempt by developed countries, mainly the United States, to

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

introduce the term *'global health security'* (GHS). It has been suggested that this should be an umbrella category for health security, organising international cooperation to counter health threats (Aldis, 2008, p. 372). As a result of 'opposition' from the aforementioned and other countries, WHO even refrained from using the term *'health* security' in the documents it adopted (Kamradt-Scott, 2018, p. 501). However, after the Ebola outbreak in 2014, the opposition of countries in the Global South both to the use of the term 'global health security' and to linking health problems to security weakened. This happened because, the Ebola outbreak began to be seen as a global crisis, as a problem exposing social inequalities within and between countries and the weaknesses of the global health governance system, but also the weaknesses of a security-conditioned approach to global health crises (Roemer-Mahler *et al.*, 2016, p. 373). During the Covid-19 pandemic, the links between the spread of the coronavirus and security were not questioned, given the number of deaths and the devastating impact on social life at the level of states and at the level of the international system.

Within the milieu of political elites, who both formulated the speech act and acted as 'public opinion', a political consensus was reached on the presentation of public health threats with the language of security (Roemer-Mahler *et al.*, 2016, p. 510). This was reflected in the decisions and actions of states and international organisations. In February 2014 The United States launched the *Global Health Security Agenda*. It was conceived as an effort by states, international organisations and civil society organisations to promote global health security, reduce threats from epidemics and promote and implement the WHO International Health Regulations (GHSA, 2022). Initiated and supported by the United States, this programme has contributed to integrating action on health security at the level of the global international system.

In summary, the process of securitisation of health risks is distinguished by several features. Firstly, it is the political actor that is the United States with its strategic preferences and the resulting structure of interests. Developed Western countries perceived epidemics primarily as a threat emerging from countries in the Global South. It was feared that, with the increasing global mobility of people, this threat could be transmitted to developed countries. The view was even formulated that securitisation – while on the one hand contributing to increasing the attention of the media, political elites and societies on health issues, increasing their funding and the actions of certain international institutions, on the other hand, meant focusing on the concerns of the 'West' and seeing the 'South' as the source of the disease threat (Weir, 2015, p. 20).

Secondly, the involvement of a political actor, political will and the associated pragmatism of interests in the securitisation of health threats has drawn attention to the interplay between the securitisation and desecuritisation of these threats. The securitisation of health threats as a side-effect, but also as a consciously pursued goal in itself, can dynamise political action on the desecuritisation of capacity, infrastructure and financial constraints on health action. A tendency towards desecuritisation occurs when existing health risks are controlled. In other words, they are resolved not as a result of emergency action, but as a result of 'normal' policy (Farrell, 2018, pp. 551–553).

Third, a feature of the securitisation of health threats is the large space of influence of the securitised phenomena and the integration of the behaviour of many actors operating at different levels of the organisation of social life, called macrosecuritisation. Critics of the securitisation mechanism have accused it of being Eurocentric in the sense of focusing on security threats existing in or concerning Europe and the actors operating here. Possibly influenced by such views, Barry Buzan and Ole Waever considered that a feature of earlier cases of securitisation was a focus on threats existing at the middle level (*middle-level*) of states and individuals. They proposed the concept of macrosecuritisation (Buzan *et al.*, 2009, p. 257). It is an overarching securitisation that encompasses, relates to and organises several middle-level securitisations. These relationships are not straightforward. Macrosecuritisation can be an intractable phenomenon and prone to centrifugal tendencies. Examples of macrosecuritisation include the Cold War, the war on terrorism, counter-piracy, epidemics and antimicrobial resistance (Yuk-pink Lo *et al.*, 2018, p. 569).

Fourthly, during the Ebola epidemic, it was noted that Western developed countries, when engaging in countering the epidemic, did not focus on the social, economic and political causes of the weakness of health systems in African countries and their asymmetric resilience against the health systems of Western countries. They focused primarily on the invention of vaccines and medicines. Without denying the importance of vaccines, the interests of Western pharmaceutical companies seem to have been important for such activities. They began to write about the *'pharmaceuticalisation'* (*pharmaceuticalisation*) of global health policy in conjunction with its securitisation. The latter, under conditions of societal concern and associated pressures of political rationality, creates a rationale for technological and pharmaceutical solutions, with a concomitant tendency to lift the restrictions previously imposed on these solutions. The view has also been formulated that the securitisation of health creates solutions that facilitate subsequent pharmaceutical responses (Roemer-Mahler *et al*., 2016, p. 376).

Fifthly, attention began to be drawn to the fact that focusing on selected health threats, such as epidemics, biological weapons, and therefore sudden, fast-spreading ones, results – as was experienced during the Covid-19 pandemic – in the creation of a kind of ranking, a hierarchy of health problems that does not reflect the real problems in this regard of the majority of the global population (DeLaet, 2014, pp. 339 ff). Concerns have been raised that prioritising diseases in this way, and from the perspective of the sense of insecurity of the populations of Global States, may lead to the neglect of other health problems, more relevant especially for countries with low and medium levels of development (Kamradt-Scott, 2018, p. 509).

SUMMARY

In summary, health security has been included in the second generation of non-military dimensions of security, conditioned more by globalisation processes than by the end of the Cold War, confirming the widening of its material scope. Reflecting the social reality, the new quality of security threats, it has simultaneously become a category of its (security) analysis. The article focuses on identifying the specificity of securitisation of health

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

threats with a focus on the concept of securitisation as a research tool, the specificity of the object of securitisation in the form of health threats and the specificity of the process of securitisation of these threats. As a result of the analysis, it was proven that the securitisation of health threats is dominated by policy actors, Western countries concerned about the cross-border spread of health threats arising in countries of the Global South. It was the politicians of Western states, mainly the United States, who formulated the speech act verbalising health threats as security threats. Despite initial opposition from countries in the Global South, under the conditions of the Ebola virus and the Covid-19 pandemic, politicians reached a global consensus on the integration of health threats into security in the broadest sense.

BIBLIOGRAPHY

Aldis, W. (2008). Health security as a public health concept: A critical analysis. *Health Policy and Planning*, *23*(6), 369–375.

Annan, K. (2009, November 9). *Problems Without Passports*. Foreign Policy.

ASEAN (2018). *ASEAN Post-2015 Helth Development Agenda 2016–2020*. ASEAN Secretariat.

Austin, J. L. (1962). *How to Do Things with Words*. Harvard University Press.

Balzacq, T. (2005). The Three Faces of Securitisation: Political Agency, Audience and Contex. *European Journal of International Relations*, *2*(11), 171–201.

Balzacq, T., & Guzzini, S. (2015). Introduction: What kind of theory – if any – is securitisation. *International Relations*, *1*(29), 97–102.

BBC (2020, 7 May). *Trump Says Coronavirus Worse 'Attack' Than Pearl Harbor*. www.bbc.com/news/world-us-canada-52568405 (03–08–2024).

BBN (2010). *NATO Strategic Concept 2010*. https://www.bbn.gov.pl/download/1/15758/conceptstrategicnanato.pdf (03–08–2024).

Binczycka-Anholcer, M., & Imiołek, A. (2011). Bioterrorism as one form of modern terrorism. *Hygeia Public Health*, *3*(46), 326–333.

Bloom, D. E., Cafiero, E. T., Jané-Llopis, E., Abrahams-Gessel, S., Bloom, L. R., Fathima, S., Feigl, A. B., Gaziano, T., Mowafi, M., Pandya, A., Prettner, K., Rosenberg, L., Seligman, B., Stein, A. Z., & Weinstein, C. (2011). *The Global Economic Burden of Non-communicable Diseases*. World Economic Forum and Harvard School of Public Health.

Bond, K. (2008). Health security or health diplomacy? Moving beyond semantic analysis to strengthen health systems and global cooperation. *Health Policy and Planning*, *23*(6), 376–378.

Bouskill, K., & Smith, E. (2019). *Global Health and Security. Threats and Opportunities*. Rand Corporation.

Bright, Ch. (1999). Invasive species: Pathogens of globalisation. *Foreign Policy*, *116*, 50–64.

Brown, L. (1977). *Redefining national security*. Worldwatch Paper 14.

Brown, T., Curto, M., & Fee, E. (2006). The World Health Organization and the transition from "international" to "global" public health. *American Journal of Public Health*, *1*(96), 62–72.

Buzan, B., & Waever, O. (2009). Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, *2*(35), 253–276.

Buzan, B., & Waever, O. (2003). *Regions and Powers*, *The Structure of International Security*. Cambridge University Press.

Buzan, B., Waever, O., & Wilde, de J. (1998). *Security. A New Framework for Analysis*. Boulder.

Caballero-Anthony, M. (2018). Health and human security challenges in Asia: New agendas for strengthening regional health governance. *Australian Journal of International Relations*, *6*(72), 602–616.

Camfield, L., & Skevington, S. (2008–2009). On Subjective Well-being and Quality of Life. *Journal of Health Psychology*, *6*(13), 764–775.

Charbonneau, B. (2021). The COVID-19 test of the United Nations Security Council. *International Journal*, *1*(76), 6–16.

Constitution of the World Health Organisation (1948). OJ., no. 61, item 477.

DeLaet, D. (2014). *Whose Interests is the Securitisation of Health Serving*? In S. Rushton, J. Youde (Eds), *Routledge Handbook of Global Health Security* (pp. 339–348). Routledge.

Dillon, M., & Lobo-Guererro L. (2008). Biopolitics of security in the 21st century. *Review of International Studies*, (34), 265–292.

Elbe, S. (2006). Should HIV/AIDS be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security. *International Studies Quarterly*, *1*(50), 119–144.

Elbe, S., Roemer-Mahler, A., & Long, Ch. (2015). Medical Countermeasures for National security: A New Government Role in the Pharmaceuticalization of Society. *Social Science and Medicine*, (131), 263–271.

Emmers, R. (2008). Securitisation. In A. Collins (Ed.), *Contemporary security studies* (pp. 109–125). Oxford University Press.

Erlanger, S. (2020). *Macron Declares France 'at War' With Virus, as E. U. Proposes 30-Day Travel Ban*. https://www.nytimes.com/2020/03/16/world/europe/coronavirus-france-macron-travel-ban.html (03–08–2024).

EU Monitor (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building a European Health Union: Increasing the EU's resilience to Cross-border health threats*. COM 724 final. https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vldpl72emsr4 (03–08–2024).

Farrell, A. M. (2018). Managing the dead in disaster response: A matter for health security in the Asia-Pacific region? *Australian Journal of International Affairs*, *6*(72), 551–566.

Fauci, A. (2007). The expanding global health agenda: A welcome development. *Nature Medicine*, *10*(13), 1169–1171.

Fidler, D. (2005). Health as Foreign Policy: Betwen Principle and Power. *Whitehead Journal of Diplomacy and International Relations*, *2*(6), 179.

Fidler, D. (2010). *The Challenges of Global Health Governance*. Council on Foreign Relations.

Fierke, K. (2010). Critical Theory, Security, and Emancipation. In R. A. Denemark, R. Marlin-Bennett (Eds), *The International Studies Encyclopedia* (vol. 2, p. 718). Wiley-Blackwell.

Foucault, M. (1998). *The History of Sexuality. Vol. 1: The will to knowledge*. Penguin.

Gannon, J. C. (2000). *The Global Infectious Disease Threat and Its Implications for the United States*. https://irp.fas.org/threat/nie99-17d.htm (01–08–2024).

GHSA, (2022). *Global Health Security Agenda: Action Packages*. https://www.cdc.gov/globalhealth/security/actionpackages/default.html (01–08–2024).

Glinski, A., & Żmuda, Z. (2020). Epidemics and pandemics of infectious diseases. *Życie Weterynaryjne*, *9*(95), 554–559.

Gostin, L., & Ayala, A. (2017). Global Health Security in an Era of Explosive Pandemic Potential. *Journal of National Security Law and Policy*, *1*(9), 53–80.

Guterres, A. (2020, April 9). *Remarks to the Security Council on the COVID-19 Pandemic*. https://www.un.org/sg/en/content/sg/speeches/2020–04–09/remarks-security-council-covid-19-pandemic (03–08–2024).

Hansen, L. (1997). A Case for Seduction? Evaluating the Poststructuralist Conceptualisation of Security. *Cooperation and Conflict*, *4*(32), 369–397.

Harman, S. (2012). *Global Health Governance*. Routledge.

Howell, A. (2014). The Global Politics of Medicine: Beyond Global Health, Against Securitisation Theory. *Review of International Studies*, *5*(40), 961–987.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Ifediora, O. F., & Aning, K. (2017). West Africa's Ebola Pandemic: Toward Effective Multilateral Responses to Health Crises. *Global Governance*, *2*(23), 225–244.

Inglehart, R. (1997). *Modernization and postmodernization: Cultural, economic, and political change in 43 societies*. Princeton University Press.

Inglehart, R. (2015). *The Silent Revolution: Changing Values and Political Styles Among Western Publics*. Princeton University Press.

Ingram, A. (2011). The Pantagon's HIV/AIDS Programmes: Governmentality, Political Economy, Security. *Geopolitics*, *3*(16) 655–674.

Jenkins, Ch., Lamazzi, M., Yeatman, H., & Borisch, B. (2016). Global Public Health: A Review and Disscussion of the Concepts Principles and Roles of Global Public Health in Today's Society. *Global Policy*, *3*(7), 332–339.

Kamradt-Scott, A. (2018). Securing Indo-Pacific health security: Australia's approach to regional health security. *Australian Journal of International Affairs*, *6*(72), 500–519.

Katz, R., & Singer, D. A. (2007). Health and security in foreign policy. *Bulletin of the World Health Organization*, *3*(85), 233–234.

Kaufman, F. X. (1970). *Sicherheit als soziologisches und socialpolitisches Problem*. Ferdinand Enke.

Kickbusch, I., Silberschmidt, G., & Buss, P. (2007). Global health diplomacy: The need for new perspectives, strategic approaches and skills in global health. *Bulletin of the World Health Organization*, *3*(85), 230–232.

Kięczkowska, J. (2019). Bioterrorism as a threat to health security. *TEKA of Political Science and International Relations*, *1*(14), 31–43.

Lowen, M. (2020), *Coronavirus: EU Could Fail over Outbreak, Warns Italy's Giuseppe Conte*. https://www.bbc.com/news/world-europe-52224838 (03–08–2024).

Lun Tian, Y. (2020). *'People's War' on coronavirus, Chinese propaganda faces pushback*. https://www.reuters.com/article/world/in-peoples-war-on-coronavirus-chinese-propaganda-faces-pushback-idUSKBN2100NQ/ (03–08–2024).

Marzęda-Młynarska, K. (2014). *Global food security governance at the turn of the 20th and 21st centuries*. Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.

Mathews-Tuchman, J. (1989). Redefining security. *Foreign Affairs*, *2*(68), 162–177.

McDonald, M. (2008). Securitisation and the Construction of Security. *European Journal of International Relations*, *4*(14), 563–587.

McInnes, C., & Williams, P. (Eds). (2008). *Health Security Studies. An Introduction*. Routledge.

Nkang, O. N., & Bassey, O. B. (2022). Securitisation of Global Health Pandemic and Reiterating the Relevance of 2005 International Health Regulations: COVID-19 and Human Security in Africa. *African Journal of Empirical Research*, *1*(3), 36–48.

OECD (2013). *Recent Trends in Official Development Assistance for Health*. OECD.

Panas, E. (2021). *Soft power of transnational civil society organisations*.

Paris, R. (2001). Human Security. Paradigm Shift or Hot Air? *International Security*, *2*(26), 87–102.

Paul, M. (2024). *COVID-19 has cost sub-Saharan Africa 13.5 million jobs in working hour losses: ILO*. https://www.downtoearth.org.in/africa/covid-19-has-cost-sub-saharan-africa-13–5-million-jobs-in-working-hour-losses-ilo-81215 (01–08–2024).

Peterson, S. (2002). Epidemic Disease and National Security. *Security Studies*, *2*(12), 43–81.

Pietraś, M. (1997). The post-Cold War security paradigm in statu nascendi. *International Affairs*, *2*, 29–52.

Pietraś, M. (2002). The essence and scope of globalisation processes. *International Affairs*, *2,* 5–34.

Pietraś, M. (2022). The category "health security" in security studies. In H. Chałupczak, K. Marzęda-Młynarska, M. Pietraś, & E. Pogorzała (Eds), *Security threats in globalisation processes. Health threats* (pp. 15–50), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej i Wydawnictwo Akademii Zamojskiej.

Pietraś, M. (2023). International health security. *Yearbook of the Institute of Central and Eastern Europe*, *21*(2), 7–34.

Pobjie, E. (2020). *Covid-19 and the scope ot the UN Security Council's mandate to address non-traditional threats to internationl peace and security*. MPIL Research Paper Series No. 41.

Price-Smith, A. (2001). *The Health of Nations: Infectious Disease, Environmental Change, and Their Effects on National Security and Development*. Mit Press.

Ray, J. (2001). Integrating Levels of Analysis in World Politics. *Journal of Theoretical Politics*, *4*(13), 355–388.

Regional Office for Europe.

Remarks to the Security Council on the COVID-19 Pandemic (n.d.). https://www.un.org/sg/en/content/sg/speeches/2020–04–09/remarks-security-council-covid-19-pandemic (03–08–2024).

Resolution 1308 (2000). Adopted by the Security Council at its 4172nd meeting, on 17 July 2000, S/RES/1308.

Resolution 2177 (2014). Adopted by the Security Council at its 7268th meeting, on 18 September 2014, S/RES/2177.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Resolution 2532 (2020). Adopted by the Security Council on 1 July 2020, S/RES/2532.

Resolution adopted by the General Assembly on 10 September 2012, A/RES/66/290.

Rockenschaub, G., Pukkila, J., & Profili, M. (2007). *Towards health security. A discussion paper on recent health crises in the WHO European Region*. World Health Organization

Roemer-Mahler, A., & Rushton, S. (2016). Introduction: Ebola and International Relations. *Third World Quarterly*, *3*(37), 373–379.

Rushton, S. (2011). Global Health Security: Security for Whom? Security from What? *Political Studies*, *4*(59), 779–796.

Searle, J. (1969). *Speech Acts: An Essay in the Philosophy of Language*. Cambridge University Press.

Security Council (2000, January 10). *The impact of AIDS on peace and security in Africa*. 4087th Meeting Monday, S/PV.4087.

Singer, D. (1961). The Level-of-Analysis Problem in International Relations. *World Politics*, *1*(14), 77–92.

Stoett, P. (2010). Framing Bioinvasion: Biodiversity, Climate Change, Governance. *Global Governance*, *1*(16), 103–120.

Stritzel, H. (2007). Towards a Theory of Securitisation: Copenhagen and Beyond. *European Journal of International Relations*, *3*(13), 357–383.

Taureck, R. (2006). Securitisation Theory and Securitisation Studies. *Journal of International Relations and Development*, *1*(9), 53–61.

UNDP (1994). *Human Development Report 1994*. Oxford University Press.

United Nations & United Nations Department of Public Information (2004). *A more secure world: Our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change*. United Nations.

United Nations (2004). *General Assembly Resolution* A /59/565.

United Nations (2020). Resolution adopted by the General Assembly on 2 April 2020, A/RES/74/270.

Waever, O. (1995), Securitisation and desecuritisation. In R. Lipschutz (ed.), *On Security* (pp. 46–87). Columbia University Press.

Wæver, O. (2004, March 17–20). *Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and their Origins between Core and Peripher'*. Paper presented at International Studies Association Conference.

Weir, L. (2015). Inventing global health security, 1994–2005. In S. Rushton, J. Youde (Eds), *The Routledge Handbook of Global Health Security* (pp. 18–31). Routledge.

WHO (2006, April 24). *Eleventh General Programme of Work, 2006–2015*. A 59/25.

Pietraś, M. (2025). Specificity of securitisation of health security risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 11–38). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Williams, M. C. (2011). Securitisation and the liverism of fear. *Security Dialogue*, *4–5*(42), 453–463.

Worldometer (2024, April 13). *COVID-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/ (31–07–2024).

Wright, I. (2021). *Are We at War? The Politics of Securitising the Coronavirus*. https://www.e-ir.info/2021/01/10/are-we-at-war-the-politics-of-securitizing-the-coronavirus/ (31–07–2024).

Youde, J. (2017). Global Health Governance in International Society. *Global Governance*, (23), 583–600.

Youde, J. (2018). The securitisation of health in the Trump era. *Australian Journal of International Affairs*, *6*(72), 535–550.

Yuk-pink Lo, C., & Thomas, N. (2018). The macrosecuritisation of antimicrobial resistance in Asia. *Australian Journal of International Affairs*, *6*(72), 567–583.

Ziętek, A. (2017). Securitisation of migration in Europe's cultural security. *Teka Komisji Politologii i Stosunki Międzynarodowych*, *3*(12), 23–42.

Małgorzata Gruchoła

Faculty of Social Sciences of the John Paul II Catholic University of Lublin, Institute of Journalism and Management
E-mail: malgorzata.gruchola@kul.pl
ORCID: 0000-0002-2367-0416

ETHICAL CHALLENGES OF USING MEDICAL ARTIFICIAL INTELLIGENCE IN THE HEALTHCARE SYSTEM

Abstract: Applications of artificial intelligence in medicine and healthcare include automated analysis of genetic data, quantification of medical images, disease prediction, telemedicine and virtual doctors, and medical robotics. The aim of the article is to identify the ethical criteria of AI in medicine and healthcare, to present the arguments for health security, to discuss the risks associated with the application of medical AI and the solutions that can mitigate them. The article confirms the research hypothesis, assuming that the application of AI technologies in medicine and healthcare implies changes in the practical, formal and systemic dimensions of healthcare, redefining the ethical principles involved.

Keywords: ethics, medicine, medical artificial intelligence, healthcare, artificial intelligence.

INTRODUCTION

The growing interest in artificial intelligence (Artificial intelligence: AI), but also concerns about its ethical use in medicine and healthcare, has been at the centre of interdisciplinary research, policy debate and social activism (Roski *et al.*, 2019; Fihn *et al.*, 2019; Chojnowski, 2020; Rudnicka *et al.*, 2020). AI technology is gradually improving the way patients are treated, access to healthcare, and optimising the way resources are

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

allocated. The potential of AI to bring about changes in healthcare (improving diagnosis, enabling increasingly personalised and precise approaches to medicine) may seem limitless (Fernández García *et al.*, 2020). The medical fields in which AI is most widely applied are clinical practice, biomedical research, public health and health administration. AI can address the healthcare challenges of an ageing population, the increase in chronic diseases, the shortage of medical staff, the inefficiency of healthcare systems, the need for sustainability with the elimination of inequalities in healthcare (European Union, 2022, pp. 4–5; European Commission. The European Pillar, 2021; European Commission, 2018; Hamed, 2020).

The application of AI in the healthcare field has both specific benefits and risks; hence, it requires a clarified set of regulatory frameworks that take into account the socio-ethical implications of its use. Indeed, the implementation of artificial intelligence raises concerns for patients, healthcare systems and society. Desired regulations include issues of clinical safety, privacy, appropriate use, fair access, as well as regulation and accountability. They raise questions about how to assess the risks and benefits of AI in healthcare, how to establish accountability in the biomedical sphere of AI and how to regulate its use, and whether AI can increase inclusion and equity in the treatment of traditionally underrepresented populations, or whether it threatens to perpetuate and increase already existing health disparities and inequalities (European Union, 2022, p. 3).

The main objective of the article is to analyse the areas where artificial intelligence can contribute to the field of medicine and healthcare, and to identify the ethical criteria for AI, along with presenting the arguments for health security. A further aim is to identify the main risks associated with the application of medical AI, and to present measures and recommendations to counter these risks. It would be a mistake and a major simplification – when attempting to evaluate AI – to limit its effects to technical aspects only. This limitation may generate techno-optimism (in Nicolas Negroponte's terms), while a personalistic perspective – which is an expression of less optimism – when confronted with the concept of so-called hard media determinism generates many questions about the role and functions of the human person (doctor, patient, pharmacist) in the healthcare system.

I adopt the research hypothesis that the application of AI technologies in medicine and healthcare implies changes in practical, formal and systemic dimensions, redefining the basic ethical principles involved: beneficence, non-maleficence, autonomy and justice. The above-mentioned changes related to AI ethics – following Maciej Chojnicki – can be attributed to three types of problems they address. The first type relates to contextualisation and operationalisation, and thus concerns the practical dimension – how to translate the values of AI medical ethics into concrete actions appropriate to the circumstances. It includes problems such as contextualisation, risk analysis, methods, tools and good practices for implementing the requirements of AI ethics into the healthcare system, how to test their implementation, etc. The second type relates to institutionalisation, i.e. formal issues, and in particular addresses questions about how to ensure compliance with AI ethics requirements. Self-regulation and legislative solutions, among others, are considered here. The last type is related to integration, and is systemic in nature. It refers to the need to consider the various impacts of AI on different areas of the healthcare system in one comprehensive analysis. This analysis should not be dispersed between separate evaluation systems (e.g, one would be based on the UN Sustainable Development Goals and the other on AI's ethical guidelines), but assumes a collective, synthetic and inclusive view of AI (Chojnacki, 2022, pp. 29–30).

To address the research problem, I rely primarily on the European Union report *Artificial intelligence in Healthcare. Applications, risks, and ethical and societal impacts*, prepared in 2022, based on a comprehensive (but non-systematic) literature review and analysis of scientific articles, recent European Union guidelines and regulations, and research on artificial intelligence. Searched keywords in literature databases, in particular Web of Science, Google Scholar and PubMed, are 'medical AI,' 'risks of AI,' 'ethical challenges of AI,' 'integrity of AI,' 'bias of AI,' 'inequality of AI,' 'impartiality of AI,' 'data privacy,' 'explainability of AI,' 'transparency of AI,' 'evaluation of AI' (European Union, 2022, p. 2).

OPERATIONALISATION AND CONTEXTUALISATION OF KEY CONCEPTS

The operationalisation of the term 'artificial intelligence' remains an ongoing methodological problem. Despite many substantive discussions and in-depth publications, no single general definition of AI has been developed (Kurp, 2023; Lambert, 2017; Iwasinski, 2023). The European Commission defines it as 'systems that exhibit intelligent behaviour by analysing their environment and taking action – with a degree of autonomy – to achieve specific goals' (European Commission, 2018, p. 2).

The classic literature on the subject – following John R. Searle – divides the field of artificial intelligence into two divisions: strong AI and weak AI. The first captures AI as "hypothetical artificial intelligent systems of a complex, or at least multitasking, nature that function autonomously in the environment, demonstrating intelligence" (Searle, 1980, p. 417). Strong AI is reserved for systems that simulate human behavioural processes (e.g. medical robots). Weak, narrow AI, on the other hand, encompasses "programs that perform specific tasks or solve specific problems that, when performed or solved by humans, are considered to require the demonstration of intelligence" (Searle, 1980, p. 417). Weak AI is thus reserved for solving specific problems (e.g. medical diagnostics).

Another term relevant to the analyses conducted is medical AI or healthcare AI. This is a type of AI that focuses on specific applications in medicine or healthcare (European Union, 2022, p. 3; Raghupathi *et al.*, 2014). Its main applications in medicine include automated analysis of genetic data, quantification of medical images, disease prediction, telemedicine and virtual doctors, and medical robotics (Fernández García *et al.*, 2020).

The next concept is the ethics of artificial intelligence, interchangeably referred to as the ethics of technology. It is considered an example of applied ethics, which – along with normative ethics that examines moral principles and norms, descriptive ethics that analyses the actual functioning of values in society, and metaethics that deals with the status of ethics and the meaning of the concepts used in it – is one of the main areas of ethics. The main aim of applied ethics is to develop practical guidelines;

these may concern various areas of human life and activity, e.g. professional ethics – medical ethics (Chojnowski, 2022, p. 14). In the case of artificial intelligence ethics, they are aimed at the people designing, using and supervising AI. AI ethics is not reduced to the mere formulation of guidelines (e.g. in the form of rules contained in codes); its important task is, among other things, to constantly critically analyse the contexts in which AI is applied and to suggest necessary adjustments – whether in the rules governing it or in the ways in which they are implemented (Chojnowski, 2022; Saja, 2015).

The ethics of artificial intelligence can be framed in various ways. M. Chojnowski distinguishes:

1. legalistic (principled, code) approach – static, focuses on formulating rules and norms and confirming compliance with them. In this view, AI ethics resembles a soft law variety. It is primarily associated with the codification stage but can also develop into an overarching approach due to the over-representation of lawyers among AI ethics experts;
2. operational (pragmatic) approach – active, seeks to apply general norms and principles in practice, i.e. to operationalise values. It involves the methodical integration of ethics into the processes of designing, implementing and using artificial intelligence;
3. critical (contextual) approach – dynamic, recognises the variety and variability of situations in which rules and norms are applied. It is associated with the stage of contextualisation. Here, ethics is a tool for critical reflection of the shape of the social and political reality in which AI operates (Chojnowski, 2022, pp. 16–17).

Currently, the legalistic approach is the most widespread. It takes the shape of recommendations or directives – either general (e.g. EU guidelines) or aimed at specific stakeholders (e.g. IEEE guidelines).

A derivative of the discussion around AI is also the dispute over whether ethics can be encoded in AI tools/technology. Advocates of the concept of Artifcial moral agents argue that this is indispensable, as AI will be used in ethically charged situations (e.g. care of the sick). Their opponents, on the other hand, emphasise that, firstly, it is impossible to speak of any real reasoning, much less moral reasoning, in relation to AI technology. Secondly – the possibility of constructing artificial moral entities is highly unlikely: AI tools/technology are not capable of moral reasoning, moreover, they do not have moral imagination, perception and reflection. Third – morality is a peculiarly human trait. Speculating about equipping AI technologies with ethics can only cloud the picture of what being a moral subject actually involves (Chojnowski, 2022, p. 13). Hence, as Aimee van Wynsberghe rightly points out, instead of fantasising about programming morality into AI, we should focus on ensuring its safe operation (van Wynsberghe & Robbins, 2019). Robots and medical software operate in ethically unobjectionable situations, but no one expects the tools to be capable of moral decisions, argues the researcher. They are simply supposed to be safe as a result of appropriate human design (Chojnowski, 2022, p. 13).

Ethicist Bernd C. Stahl (2021) lists three main types of challenges related to artificial intelligence. These are:

1. machine learning issues,
2. social and political issues of living in a digitised world,
3. metaphysical questions about the nature of man and the status of machines.

The first group covers technical issues directly related to the specifics of machine learning, including discrimination as an effect of algorithmic *bias*. It results from training AI systems on insufficiently representative data sets. As a result, AI can act unfairly towards certain groups of people (e.g. people with a rare disease). Another problem is the opaqueness of the operation of AI, evident in so-called ‘black boxes,’ i.e. AI systems in which the way to arrive at certain results remains incomprehensible even to those responsible for programming them. In such situations, the decisions made by AI are sometimes arbitrary because we do not know the criteria that would justify them. This is unacceptable for applications that affect important spheres of human life, such as healthcare. Another example from this category is the ability to discover relationships between seemingly neutral data (so-called correlation), which can generate privacy and data protection risks. AI systems – with a sufficiently large data pool – are able to extract sensitive data, information about patients who have not publicly disclosed it themselves (Chojnowski, 2022, pp. 10–11).

The problems in the second group of challenges relate to the impact of AI systems on various spheres of social and political life. They include, among others, the disappearance of various professions as a result of advanced automation (medical analyst, diagnostician), the declining sense of agency among workers increasingly treated as an adjunct to medical robots and AI technologies, the issue of concentration of capital and power by major pharmaceutical and technology companies, monopolising digital services in the global market (AI applied to the production of new drugs), and the growing risk of mass surveillance (Chojnowski, 2022, p. 11; Strubell *et al.*, 2019).

The third group of issues concerns the moral and legal status of AI (as well as the human condition). In addition to issues about the potential rights and responsibilities of embodied artificial intelligence, it includes an assessment of the implantation of neurotechnology solutions into the human body to enhance human cognitive or perceptual functions (Stah, 2021). It covers issues related to the functioning of technology connected to the human body (exo-enhancement), technology in the body (endo-enhancement), and problems related to the integration of technology into the human body for its complementation (techno-enhancement, i.e. prosthesis) and/or extension (techno-enhancement, i.e. implantation) of the human being. This links to the process of implanting the human body with various chips connected to the nervous system, providing the possibility to experience various technonics, e.g. direct communication with a computer or technostimulation of the nervous system (see Gruchoła, 2019a, 2019b).

The identification of the above problem groups does not imply that they need to be considered in isolation. As Mark Coeckelbergh (2020, p. 38) notes, they are interrelated. The context of the AI discussion is very broad. Its backdrop is formed by deep disputes about the nature of human beings, their consciousness and mind, as well as about understanding, creativity, meaning or knowledge (Chojnowski, 2022, p. 11).

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

INSTITUTIONALISING HEALTH SYSTEM COMPLIANCE WITH AI ETHICS REQUIREMENTS

Discussions around artificial intelligence are as much about the technology itself as they are about humans. Hence, AI is increasingly being treated not as an abstract or self-contained entity but as part of wider social life, also taking into account the institutionalisation of the healthcare system. The questions arise: what are the arguments for the need for ethical AI in medicine and healthcare? Furthermore, why does the medical business need ethics?

Aniela Dylus (2023) proposes the following typology of arguments supporting the need for ethics in business, which I propose to adapt also to medical institutions:

1. Semblance of ethics:
   - hypocrisy strategy,
   - enforcing ethics,
   - ethical business as a manifestation of... escape from ethics.
2. Pragmatic (utilitarian) reasons:
   - higher competitiveness of "ethical companies,"
   - a dam for moral erosion.
3. Personalistic rationale:
   - an anthropocentric teleology of business,
   - civilisation rationale,
   - the culture-building function of 'ethical business.'

The 'sham of ethics' consists of a 'strategy of hypocrisy,' 'forcing ethics' and 'ethical business as an escape from ethics.' The essence of the "strategy of hypocrisy" boils down to the fact that "while praising and recommending the benefits of solidarity and cooperation, the player himself does not follow his own recommendations, thus enabling the optimal situation for himself – where the partner follows his advice" (Dylus, 2023). "Enforcing ethics" is pressure from NGOs and the media to follow certain rules. Moreover, in a situation of deep crisis of morality and the abandonment of really important existential questions, particularistic ethics give people a deceptive sense of abiding by ethics (Dylus, 2023).

Pragmatic (utilitarian) arguments recognise the "higher competitiveness of 'ethical companies.'" Business ethics are seen as an effective method of competitive struggle that avoids bankruptcy;

as an instrument for increasing profit; as one of the premises in companies' strategies and thus – as a 'key element of marketing.' Moreover, the 'aestheticisation' of the activities of large corporations is an understandable attempt by the business community to defend itself against moral destruction. The tarnishing of an image, the tarnishing of a good name, the loss of trust by one company, in a way, hits the whole environment. Ethics thus provides a 'dam for moral erosion' (Dylus, 2023).

The third group of arguments – personalistic – includes an anthropocentric teleology of business, civilisational rationales and the culture-creating function of 'ethical business.' The anthropocentric teleology of business emphasises the accentuation of man's subjectivity in social life, his priority over things. The rationales of civilisation, generated by the rapid progress of science and technology, place the participants in economic processes more and more often in completely new situations. They are sometimes confronted with moral dilemmas that no one has resolved before (e.g. diagnoses formulated by artificial intelligence). Ethical standards in the medical business should be seen as a factor supporting the healthcare system in its culture-building function. They are an expression of people's realisation of their responsibility for the future. This rationale for 'ethical business' is sometimes succinctly described as: "time for responsibility" (Dylus, 2023), primarily in medicine and healthcare.

ETHICAL IMPLICATIONS OF MEDICAL ARTIFICIAL INTELLIGENCE IN TERMS OF PREDICTING THREATS – A SYSTEMIC PERSPECTIVE

In 1970, William B. Schwartz stated that 'information technology is likely to exert its major influence in augmenting, and in some cases substantially replacing, the intellectual functions of the physician' (Schwartz, 1970, p. 1257). Despite the passage of more than 50 years, Schwartz's prediction has yet to be fully realised. Initial results of AI applications are not as robust as predicted and it is difficult to assess its actual impact (Roski *et al.*, 2019; Fihn *et al.*, 2019). Some researchers argue that the capabilities of medical AI as a whole have been greatly overestimated; moreover, there is no data showing real improvements in patient outcomes (Angus, 2020).

Other experts explicitly express concerns about the potential negative consequences of medical AI, including clinical, technical and socio-ethical risks (Gerke & Cohen, 2020; Morley & Floridi, 2020; Manne & Kantheti, 2021; European Union, 2022, p. 15). In the report *Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts* identified the main risks of AI in medicine and healthcare. These are:

1. patient harm caused by artificial intelligence errors,
2. inappropriate use of biomedical artificial intelligence tools,
3. bias of artificial intelligence and the perpetuation of existing inequalities,
4. lack of transparency,
5. privacy and security issues,
6. accountability gaps (European Union, 2022, pp. 15–28).

The negative effects of the above risks are minimised by adhering to the ethical principles of AI. The ethical principles underlying the EU's concept of trustworthy AI are derived from the Universal Declaration of Human Rights, the fundamental rights, i.e. respect for human dignity, individual freedom, respect for democracy, justice and the rule of law, equality, non-discrimination and solidarity, and respect for citizens' rights. These are: transparency, inclusion, accountability, impartiality, credibility, security and privacy (see Gruchoła, 2024; The 'Good' Algorithm, 2021). Firstly, artificial intelligence must be transparent; that is, the way the system works should be understandable to users. Secondly, inclusive; AI systems must not discriminate against anyone, e.g. on the basis of race, colour or religion. AI systems must not mimic or create prejudice. Behind each AI system must be a person or organisation that can be held accountable for its actions, and the systems themselves must be trustworthy. Furthermore – AI must be safe for users and respect their privacy.

According to Maciej Chojnowski (2022) these are:

1. the principle of *respect for human autonomy*,
2. *the prevention of harm* principle,
3. the principle of justice (*fairness*),
4. the principle of *explicability.*

They fit into the four basic principles of healthcare ethics: autonomy, non-harm, justice and beneficence.

According to the first principle – respect for human autonomy – interaction with AI systems must provide people with the possibility of self-determination. Its implementation requires *human agency and oversight* (*human agency and oversight*). It includes activities such as assessing the fundamental rights implications of AI, providing users with the knowledge and tools to understand and interact with AI systems, and putting in place governance mechanisms to ensure human oversight of AI (Chojnacki, 2022, p. 20).

An example of the risks associated with AI in medicine and healthcare is the inappropriate use of biomedical artificial intelligence tools. It can result in an incorrect medical assessment and thus decision, and consequently potential harm to the patient. Potential causes of inappropriate use of AI include limited physician and patient involvement in AI development (Quaglio *et al*., 2019), lack of AI training among healthcare professionals (Gillespie *et al*., 2021), proliferation of readily available medical AI applications, medical knowledge on the Internet without sufficient explanation and information (Freeman *et al*., 2020).

Among the possible ways to reduce human error or misuse of future medical AI solutions, the following are recommended: a user-centred AI concept (AI usability testing); the future integration of AI education into the core curriculum of schools at all levels of education; new media competence programmes to increase public awareness of AI; and informing doctors and patients about new AI technologies (European Union, 2022, p. 19).

According to principle two – *prevention of harm* – AI systems must be safe and secure. Its implementation presupposes:

- *technical robustness* and safety of AI (*technical robustness and safety*). Refers to the robustness of AI systems against attack, having a contingency plan and procedures to assess the potential risks of using AI in different areas, a clear AI system development and evaluation process to reduce and correct the risk of inaccurate predictions, *reliability* and *reproducibility* of AI processes to assess whether the system performs correctly with different inputs (and in different situations), and whether it behaves identically in an experiment repeated under the same conditions;
- *privacy and data governance*. It sets out requirements for the protection of privacy and personal data throughout

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

the lifecycle of an AI system, the quality and integrity of data (including appropriate testing and documentation processes), and the development of protocols that define access to data (Chojnacki, 2022, pp. 20–21).

Examples of risks linked to the principle under review are patient harm caused by AI errors and lack of privacy and data protection.

The main causes of AI errors are noise and artefacts in AI input data and clinical measurements (Pinto *et al*., 2013), data shift between AI training data and real data (Subbaswamy *et al*., 2020), and unexpected differences in clinical contexts and environments (Ellahham *et al*., 2020).

The medical consequences of such errors can include misdiagnosis of life-threatening conditions and false diagnosis, leading to inadequate treatment and planning or prioritisation of interventions (European Union, 2022, p. 15).

The proposed remedies include:

– comprehensive, multi-centre study to evaluate and validate regulatory artificial intelligence solutions;
– AI algorithms are designed and deployed as enablers (as opposed to fully autonomous tools) and identifiable and dynamic (equipped with mechanisms to continue learning from new scenarios and errors detected in practice). This aspect requires a degree of human control and vigilance to identify emerging issues;
– infrastructural and technical changes to enable regular updates of AI (based on past and new training), as well as the implementation of regulations to ensure the integration of such mechanisms in healthcare facilities (European Union, 2022, p. 17).

The development of artificial intelligence technologies in healthcare has highlighted the potential risks associated with the lack of privacy, confidentiality and protection of patient and citizen data. The main risks in the scope analysed are the sharing of personal data without the patient's fully informed consent, the repurposing of data without the patient's knowledge, data breaches that may expose sensitive or personal data, and the risk of harmful – and even potentially fatal – cyber attacks on AI solutions, whether at the individual, hospital or health system level (European Union, 2022, pp. 24–25; Vyas *et al*., 2020; Koops, 2021).

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The recommended remedies are to increase patients' awareness and skills regarding privacy and security risks, as well as informed consent and cyber security. In addition, legislation must protect citizens from data breaches and diversion. A decentralised, federated approach to artificial intelligence should be promoted to harness the power of large datasets from clinical sites without the need for dangerous data transfers. The security of cloud-based systems should be improved and AI algorithms should be protected from cyber attacks (European Union, 2022, p. 25).

The third principle – *fairness* – relates to both substantive and procedural justice. The requirements to implement it and achieve ethical AI are:

– diversity, *non-discrimination and fairness*, which includes, inter alia, avoiding unfair *bias* during the training and use of AI systems; ensuring diversity of opinion by including in the design of AI people from different backgrounds, professions and fields and stakeholders who would be directly or indirectly affected by the system; soliciting regular feedback from AI users (Chojnacki, 2022, p. 20);
– *societal and environmental wellbeing*, which points, among other things, to the need to create sustainable and environmentally friendly artificial intelligence by controlling the development, implementation and use of AI systems, as well as the entire supply chain; to monitor and take into account in the design, implementation and use of AI systems their impact on society in various areas, including the institutions of the democratic state;
– *accountability*, which includes the need to ensure *auditability of* algorithms, data and design processes; to conduct *impact* assessments of AI systems, both before and during their development, implementation and use; to provide a mechanism for reporting erroneous AI decisions and responding to negative consequences; to develop trade-offs between the above principles in situations of possible conflicts between them and to evaluate these trade-offs in view of the risks to ethical principles (Chojnacki, 2022, pp. 20–21).

Linked to the principle of fairness is the risk of bias in medical AI and the perpetuation of inequality. Biases based on gender, race, ethnicity, age, socio-economic status, geographic location and place of residence are common in AI models (European Union, 2022, p. 20; Hoffman *et al*., 2016). The most common causes of AI biases stem from biased and inappropriate datasets based on structural biases and systemic discrimination, the ways in which data are collected, disparities in access to high-quality digital equipment and technologies, and lack of diversity and interdisciplinarity in technological, scientific, clinical and decision-making teams (Ghassemi, 2021).

The recommended remedy is for AI developers to take greater care in accurately selecting and labelling the data and variables to be used when training the models. These should be representative and balanced in terms of key attributes such as gender, age, socio-economic conditions, ethnicity, and place of residence. It is also recommended to involve sociologists and biomedical ethicists in the development teams, in addition to data scientists and expert researchers (European Union, 2022, p. 22).

Also linked to the principle of fairness is the threat of loopholes for 'algorithmic accountability' in healthcare. While this term may refer to the task of holding the algorithm itself accountable, it is in fact quite the opposite: it emphasises the fact that algorithms are created through a combination of machine learning and human design, and that errors or misconduct in algorithms come from humans developing, implementing or using AI technologies, especially as AI systems themselves cannot be held morally or legally accountable (Raji, 2020). Current limitations to AI accountability include:

1. legal gaps in existing national and international laws, which still do not allow for clear definitions of medical AI liability and responsibility;
2. difficulties in defining the roles and responsibilities of the many actors involved in medical AI;
3. lack of ethical and legal governance for AI producers and industry (European Union, 2022, p. 26; WHO, 2021).

Challenges in adapting current law and ethical responsibility rules to new applications of AI include: (1) the problem of multiple actors involved in the development, implementation and use of medical AI (e.g., AI developers, data managers, physicians, patients, healthcare providers), which makes it difficult to determine the extent of their responsibility; (2) the difficulty in determining the exact cause of any AI-related medical error, which may be due to the AI algorithm, the data used to train it or its misuse and understanding in clinical practice; and (3) the multiplicity of governance frameworks and the lack of standardised ethical and legal standards in AI industries.

Proposed ways to address the current lack of accountability in medical AI include: the implementation of procedures to define the responsibilities of AI developers and clinical users in situations where AI-assisted medical decisions harm patients; and the creation of regulatory agencies for medical AI to develop and enforce a single regulatory framework to ensure accountability of actors, including AI manufacturers (European Union, 2022, pp. 26–27).

The final, fourth principle – *explainability* – requires that the processes involved in AI systems are transparent, while the potential and goals are communicated explicitly. *Transparency* refers, among other things, to the *traceability* of data sets, processes and algorithms used by AI to make decisions, which facilitates *auditability*; *explainability* adapted to the level of knowledge of stakeholders in situations where the AI system has a significant impact on people's lives; explicit communication of information that users are dealing with the AI system (Chojnacki, 2022, pp. 20–21).

A significant threat to the healthcare system is the lack of transparency in the design, development, evaluation and implementation of medical AI tools. AI transparency is closely linked to the concepts of traceability and explainability, which correspond to two distinct levels at which it is required: (1) transparency of the processes of AI development and use (traceability) and (2) transparency of the AI decisions themselves (explainability) (Yang *et al.*, 2021).

Specific risks associated with a lack of transparency in biomedical AI include a lack of understanding and trust in the predictions and decisions generated by the AI system, difficulties in independently replicating and evaluating AI algorithms, difficulties in identifying sources of AI errors and determining who and/or what is responsible for them, and limited use of AI tools in clinical practice and real-world settings.

A number of opportunities are available to improve the transparency of AI technologies in healthcare. These include the introduction of an 'AI passport' to document all key model information, the development of traceability tools to monitor the use of AI algorithms once they have been deployed (e.g. logging potential errors), and the recognition by regulators of the traceability and reliability of AI tools as a prerequisite for their certification (European Union, 2022, p. 23).

SUMMARY

The research hypothesis assuming that the application of AI technologies in medicine and healthcare implies changes in the practical, formal and systemic dimensions of healthcare, redefining the basic ethical principles therein was verified positively.

The use of healthcare AI in actual clinical practice generates obstacles to integrating new AI tools with those already in place. These include: 1. limited data quality, structure and interoperability across disparate clinical sites and electronic medical records; 2. potential changes in the doctor-patient relationship due to the introduction of AI medical tools and increased, under-regulated access to patient data; 3. lack of clinical and technical integration and interoperability of AI tools with existing clinical procedures and electronic healthcare systems (Fihn *et al.*, 2019; Nagendran *et al.*, 2020).

The introduction of artificial intelligence technology into daily practice generates practical, technical and clinical implications for both clinicians and patients. It is unclear whether medical AI tools will be systematically implemented in different clinical centres and health systems and whether they will be compatible with existing clinical and technical information and data workflows (Meskó & Görög, 2020) without significant modifications to existing clinical practices, care models and even training programmes. AI vendors, in collaboration with health system professionals, will need to establish standard operating procedures for all new AI tools to ensure their interoperability across clinical sites and integration in heterogeneous electronic healthcare systems. In particular, new AI tools need to be developed, ensuring their future compatibility and communication with already existing technologies such as genetic sequencing, electronic patient records and e-health consultations (European Union, 2022, p. 28–29; Arora, 2020).

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The rapid development of medical artificial intelligence will require frequent updating of the operationalisation and contextualisation, institutionalisation and integration of the values of AI ethics into new actions and circumstances in healthcare. These actions should lead to – to quote Archbishop V. Paglia – 'the humanisation of technology rather than the technologisation of man' (Wittenberg, 2023).

BIBLIOGRAPHY

Angus, D. C. (2020). Randomized clinical trials of artificial intelligence. *JAMA*, *323*(11), 1043–1045.

Arora, A. (2020). Conceptualising Artificial Intelligence as a Digital Healthcare Innovation: An Introductory Review. *Med Devices (Auckl)*, *3*, 223–230. https://doi.org/10.2147/MDER.S262590

Chojnowski, M. (2021). *Poles and technology: Only the future is threatening*. https://ethicstech.eu/polacy-i-technologie-tylko-przyszlosc-jest-grozna/

Chojnowski, M. (2022). *The ethics of artificial intelligence.* Centre for Ethics in Technology of the Humanites Institute.

Coeckelbergh, M. (2020). *AI Ethics*. The MIT Press.

Dylus, A. (2023). *"Why business needs ethics?" VII Festival of Catholic Social Teaching: 29.09.2023*. YouTube. https://www.youtube.com/live/4T8TQ5bqHmw?app=desktop.

Ellahham, S., Ellahham, N., & Simsekler, M. C. E. (2020). Application of artificial intelligence in the health care safety context: Opportunities and challenges. *American Journal of Medical Quality*, *35*(4), 341–348.

European Commission (2018). *Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Artifcial Intelligence for Europe*. COM 237 fnal.

European Commission (2021). *The European Pillar of Social Rights in 20 principles*. https://employment-social-affairs.ec.europa.eu/policies-and-activities/european-pillar-social-rights-building-fairer-and-more-inclusive-european-union/european-pillar-social-rights-action-plan_en

European Union (2022). *Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts. PE 729.512*. European Parliamentary Research Service. http://www.europarl.europa.eu/stoa (29–02–2024).

Fernández García, J., Spatharou, A., Hieronimus, S., Beck, J. P., & Jenkins, J. (2020). *Transforming healthcare with AI: The impact on the*

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

workforce and organisations. Executive summary. EIT Health & McKinsey & Company.

Fihn, S. D., Saria, S., Mendonça, E., Hain, S., Matheny, M., Shah, N., Liu, H., & Auerbach, A. (2019). *Deploying AI in clinical settings. In artificial intelligence in health care: The hope, the hype, the promise, the peril*. National Academy of Medicine.

Floridi, L. (2011). Enveloping the world: the constraining success of smart technologies. In I. Mauger (Ed.), *CEPE 2011*: *Crossing Boundaries. Ethics in Interdisciplinary and Intercultural Relation*. (pp. 111–116), https://coeckelbergh.fles.wordpress.com/2015/03/48.pdf

Freeman, K., Dinnes, J., Chuchu, N., Takwoingi, Y., Bayliss, S. E., Matin, R. N., Jain, A., Walter, F. M., Williams, H. C., & Deeks, J. J. (2020). *Algorithm-based smartphone apps to assess risk of skin cancer in adults: Systematic review of diagnostic accuracy studies*. BMJ.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In A. Bohr, K. Memarzadeh (Eds), *Artificial intelligence in healthcare* (pp. 295–336). Academic Press.

Gillespie, N., Lockey, S., & Curtis, C. (2021). *Trust in Artificial Intelligence: A Five Country Study*. The University of Queensland and KPMG Australia.

Gómez-González, E., Gómez, E. (2020). *Artificial Intelligence in medicine and healthcare: Applications, availability and societal impact. EUR 30197 EN*. Publications Office of the European Union.

Gruchoła, M. (2019a). Technological "Extensions" of the Body and the Value of the Human Body. *Zeszyty Naukowe KUL*, *62*(3), 15–33. https://doi.org/10.31743/zn.2019.62.3.02

Gruchoła, M. (2019b). The Machine in the Body – the Body in the Machine: Perception of the Human Body in a Post-Biological Society. *Cultural Studies Yearbooks*, *10*(3), 27–44. http://dx.doi.org/10.18290/rkult.2019.10.3–2

Gruchoła, M. (2024). *"Interreligious cooperation among ethicists around issues of artificial intelligence," Ethics in Media series*. Pontifical University of John Paul II. (Accepted for publication.)

Hamed, S., Thapar-Björkert, S., Bradby, H., & Ahlberg, B. (2020). Racism in European Health Care: Structural Violence and Beyond. *Sage Journals*, *30*(11), 1662–1673.

Hoffman, K. M., Trawalter, S., Axt, J. R., & Oliver, M. N. (2016). Racial bias in pain assessment and treatment recommendations, and false beliefs about biological differences between blacks and whites. *Proceedings of the National Academy of Sciences*, *113*(16), 4296–4301.

Iwasinski, Ł. (2023). Can the law keep up with the development of artificial intelligence. In B. Sosińska-Kalata, P. Tafiłowski (Eds), *Information science in a period of change. Science in the face of modernity: Information wars* (pp. 49–58). Association of Polish Librarians.

Koops, B. J. (2021). The concept of function creep. *Law, Innovation and Technology*, *13*(1), 29–56.

Kurp, F. (2023). *Artificial intelligence from scratch*. Helion Publishing House.

Lambert, P. (2017). Computer-Generated Works and Copyright: Selfes, Traps, Robots, AI and Machine Learning. *European Intellectual Property Review*, *39*, 12–20.

Manne, R., & Kantheti, S. C. (2021). Application of artificial intelligence in healthcare: Chances and challenges. *Current Journal of Applied Science and Technology*, *40*(6), 78–89.

Morley, J., & Floridi, L. (2020). An ethically mindful approach to AI for health care. *Lancet*, *395*, 254–255.

Nagendran, M., Chen, Y., Lovejoy, C. A., Gordon, A. C., Komorowski, M., Harvey, H., Topol, E. J., Ioannidis, J. P. A., Collins, G. S., & Maruthappu, M. (2020). Artificial intelligence versus clinicians: Systematic review of design, reporting standards, and claims of deep learning studies. *BMJ*, *368*, 689–693.

Paglia, V., & Pegoraro, R. (2021). *The 'Good' Algorithm? Artificial Intelligence Ethics, Law, Health. Proceedings of the XXVI General Assembly of Members*. Pontifical Academy for Life.

Pinto, A., Pinto, F., Faggian, A., Rubini, G., Caranci, F., Macarini, L., Genovese, E. A., & Brunese, L. (2013). Sources of error in emergency ultrasonography. *Critical Ultrasound Journal*, *5*(1), 1–24.

Quaglio, G. L., & Boone, R. (2019). *What if we could fight drug addiction with digital technology?* EPRS, European Parliament.

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health information science and systems*, *2*(1), 1–10.

Raji, I. D. (2020). *Closing the AI Accountability Gap: Defining an End-to--End Framework for Internal Algorithmic Auditing*. Publication History.

Roski, J., Chapman, W., Heffner, J., Trivedi, R., Del Fiol, G., Kukafka, R., Bleicher Estiri, O. H., Klann, J., & Pierce, J. (2019). How artificial intelligence is changing health and health care. In M. Matheny, S. T. Israni, M. Ahmed, D. Whicher (Eds), *Artificial Intelligence in Health Care: The hope, the hype, the promise, the peril* (pp. 7–36). National Academy of Medicine.

Rudnicka, A., Kaczorowska-Spychalska, D., Kulik, M., & Reichel, J. (2020). *Digital ethics – Polish consumers towards ethical challenges related to the development of technology*. I Ogólnopolski Raport. https://wydawnictwo.uni.lodz.pl/wp-content/uploads/2021/01/Digital_ethics_raport.pdf

Gruchoła, M. (2025). Ethical challenges of using medical artificial intelligence in the healthcare system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 39–58). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Saja, K. (2015). *Normative ethics. Between consequentialism and deontology.* Wydawnictwo Uniwersytetu Łódzkiego.

Schwartz, W. B. (1970). Medicine and the computer: The promise and problems of chang. *N Engl J Med*, *283*(23), 1257–1264.

Searle, J. R. (1980). Minds, brains, and programs. *The Behavioral and Brain Sciences*, *3*, 417–423.

Seyyed-Kalantari, L., Liu, G., McDermott, M., Chen, I. Y., & Ghassemi, M. (2021). CheXclusion: fairness gaps in deep chest X-ray classifiers. In B. Russ, A. Altman, K. Dunker, L. Hunter, M. D. Ritchie, T. Murray, T. E. Klein (Eds), *BIOCOMPUTING 2021: Proceedings of the Pacific Symposium* (pp. 232–243). World Scientific Publishing.

Stahl, B. C. (2021). *Artificial Intelligence for a Better Future. An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies*. Springer Cham. https://doi.org/10.1007/978–3-030–69978–9

Strubell, E., Ganesh, A., & McCallum, A. (2019). *Energy and Policy Considerations for Deep Learning in NLP.* Cornell University. https://doi.org/10.48550/arXiv.1906.02243

Subbaswamy, A., & Saria, S. (2020). From development to deployment: Dataset shift, causality, and shift-stable models in health AI. *Biostatistics*, *21*(2), 345–352.

van Wynsberghe, A., & Robbins, S. (2019). Critiquing the Reasons for Making Artificial Moral Agents. *Sci Eng Ethics*, *25*, 719–735. https://doi.org/10.1007/s11948–018–0030–8

Vyas, D. A., Eisenstein, L. G., & Jones, D. S. (2020). Hidden in Plain Sight – Reconsidering the Use of Race Correction in Clinical Algorithms. *The New England Journal of Medicine*, *383*, 874–882.

Wittenberg, A. (2023, January 11). *Catholics, Jews and Muslims want ethical artificial intelligence*. Dziennik.pl. https://technologia.dziennik.pl/aktualnosci/artykuly/8632545,religia-technologie-etyka-katolicy-zydzi-muzulmanie-swiat-dgp.html (01–03–2024).

World Health Organization (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*. https://www.euro.who.int/en/health-topics/noncommunicable-diseases/mentalhealth/news/news/2012/10/depression-in-europe/depression-in-europe-facts-and-figures

Yang, G., Ye, Q., & Xia, J. (2021). *Unboxing the Black box for the Medical Explainable AI via Multi-modal and Multicentre Data Fusion: A Mini-Review, Two Showcases and Beyond*. Elservier.

Katarzyna Marzęda-Młynarska

Faculty of Political Science and Journalism of the Maria Curie-Skłodowska University,
Institute of International Relations UMCS
E-mail: katarzyna.marzeda-mlynarska@mail.umcs.pl
ORCID: 0000-0002-4608-7290

CHALLENGES AND PROSPECTS FOR INTERNATIONAL FOOD SYSTEMS IN THE LIGHT OF THE COVID-19 PANDEMIC EXPERIENCE

Abstract: The COVID-19 pandemic significantly impacted international food systems, exposing their weaknesses and subjecting them to various disruptions. Issues related to the pandemic affected all dimensions of food production, processing, distribution, and consumption worldwide. The negative effects of the pandemic contributed to disruptions in global supply chains, changes in consumption patterns, and production declines. This article aims to analyse the challenges and prospects for international food systems in the context of the COVID-19 pandemic experiences, including impacts on food security, resilience to unforeseen events, and technological innovations. The article is based on the analysis of reports from international organisations and scientific articles.

Keywords: COVID-19 pandemic, international food systems, supply chains, food security, technological innovations, sustainable agriculture, crisis resilience.

INTRODUCTION

The COVID-19 pandemic had a huge impact on almost all aspects of social, economic and political life around the world. Coronavirus infections led to severe restrictions on movement, border closures and social isolation, which had a direct impact on global mobility

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

and trade. As a result, supply chains have been disrupted, causing problems with the availability of many products, including food. In the economic sphere, the pandemic caused the greatest economic crisis since the Second World War. Many companies, especially small and medium-sized ones, had to close their operations, leading to an increase in unemployment on an unprecedented scale.

In a particular way, the Covid-19 pandemic exposed and exacerbated existing social inequalities, both globally and locally. Globally, as with previous crises, the poorest countries, including those that base their economies on sectors such as tourism, raw material exports and agriculture, have been most adversely affected. The collapse of these sectors as a result of, among other things, disruptions in supply chains, falling global demand, labour shortages (agricultural sector), as well as price fluctuations and financial constraints, has led to a decline in national incomes, rising unemployment and poverty.

One of the most noticeable effects of the Covid-19 pandemic was the challenges that the increase in infections, as well as the sanitary policies implemented by states, posed to systems of existential importance, such as the health system and the food system. Particularly in the case of the latter, the empty shelves in shops and the Dantean scenes played out in supermarkets, accompanying customers trying to stock up on food, have risen to symbolic status.

The purpose of this article is to analyse the challenges and prospects for international food systems as a result of the experience of the Covid-19 pandemic. In doing so, it should be noted that for the purposes of the article, the FAO definition of food systems is adopted, according to which they are:

> [...] the entire range of value-adding actors and their interrelated activities involved in the production, collection, processing, distribution, consumption and utilisation of food products. Food systems encompass all food products from crop and livestock production, forestry, fisheries and aquaculture, as well as the wider economic, social and natural environment in which these diverse production systems are embedded. (FAO, 2024)

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The article is structured in three parts that will successively analyse, firstly, the impact of the Covid-19 pandemic on international food systems, including disruptions to supply chains, changes in food demand and supply, and the impact on farmers and food producers. Second, the challenges that the pandemic has posed to international food systems, primarily in terms of food security, resilience to unpredictable 'black swan' phenomena (Taleb, 2020), which include Covid-19, and innovation and new technologies. Thirdly, the prospects for international food systems, including demands for shorter supply chains, demands for greater food self-sufficiency, or changes in agricultural policies within countries and at the global level.

The article was prepared using the desk research method and is mainly based on an analysis of reports from international organisations and research institutes such as FAO, WFO, IFPRI and scientific articles available in Web of Science and Scopus databases.

IMPACT OF THE COVID-19 PANDEMIC ON INTERNATIONAL FOOD SYSTEMS

The Covid-19 pandemic has had a significant impact on international food systems (Dury *et al.*, 2020), exposing their weaknesses and exposing them to a variety of disruptions. The associated problems have affected all dimensions of food production, processing, distribution and consumption around the world. The negative effects of the pandemic on international food systems have taken the form, firstly, of disruptions to global supply chains, resulting in supply delays and shortages of certain products. Secondly, changes in food consumption patterns, as a result of the closure of restaurants, schools and hotels operating on a mass catering model, which affected food demand and supply. Thirdly, periodic declines in production and reductions in forms of food marketing, as a consequence of lockdown policies, restrictions on labour mobility and increases in contamination.

The first and most immediate impact of the pandemic was the disruption of global food supply chains (Wróbel, 2024). Restrictions imposed around the world in the form of lockdowns, and restrictions on movement, including those associated with

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

periodic border closures, affected the ability to produce, process and distribute food. Labour shortages due to disease or travel restrictions have led to reduced yields and delays in foodsupplies. In many countries, food producers had to cope with sudden changes in the availability of seasonal workers, adding to logistical problems. The Covid-19 pandemic particularly affected migrant workers, who play a key role in the agricultural sector of many countries. For example, a shortage of workers from Eastern Europe caused crops such as asparagus to rot in fields in Western European countries because there was no one to harvest them (E-vegetables, 2020).

The Covid-19 pandemic also caused major disruptions in food logistics and transport. Border restrictions introduced by countries, e.g. in the form of testing or increased sanitary--epidemiological controls, together with reduced air traffic, have affected the international transport of fresh produce, which has significantly increased logistics costs. In addition, export restrictions introduced by countries (e.g. Russia, Kazakhstan, India or Turkey) to secure domestic food stocks have contributed to the destabilisation of food markets and consequently increased food prices on international markets (Zhou & Delgado, 2020).

Disruptions in global supply chains have not been without impact on the food industry. Many processing plants have had to reduce or suspend operations, whether due to restrictions in the supply of agricultural raw materials, safety measures being introduced or, finally, a shortage of workers. An example of this was the situation in the United States, where the largest US dairy cooperative, Dairy Farmers of America, was forced to ask farmers to pour their milk because of logistical problems and transport restrictions (Huffstutter, 2020).

Disruptions in global supply chains have particularly affected low-income countries heavily dependent on food imports. Indeed, export restrictions imposed by food producers have led to rising food prices, which, combined with import restrictions and panic buying, have exacerbated the problem of hunger and malnutrition in regions such as sub-Saharan Africa and the Middle East (Zhou & Delgado, 2020).

The fragility of global food supply chains in the face of a pandemic also had an impact on food demand and supply. The changes

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

observed were both micro and macro. In the first case, there was a significant shift in demand from the service sector: hotels, restaurants, catering, to retail. Consumers began to stockpile food, which led to a temporary increase in demand for long-lasting products such as flour, pasta, canned goods and other products with a long shelf life. In many cases, supermarkets have had to place restrictions on the purchase of certain products to prevent them from running out. Paradoxically, therefore, the retail chains were experiencing an increase in sales, but at the same time, due to disruptions in the supply chain, they were facing product shortages and supply problems. On the other hand, restrictions due to sanitary policies forced the introduction of innovations and new technologies into the food trade. In particular, the lockdown-related increase in consumer interest in online shopping has forced companies to accelerate investment in e-commerce development (Felix *et al.*, 2020).

On a macro level, the Covid-19 pandemic overlapped with existing problems, such as climate change, which were already affecting agricultural production. For example, droughts in some regions of the world further reduced food supply during the pandemic (Mishra *et al.*, 2021). Not me less important were the effects of export restrictions imposed by leading food producers such as India and Russia (Kowalska *et al.*, 2022). Clearly, however, the Covid-19 pandemic has significantly accelerated the growth of the online food sales market worldwide. The global online food delivery market is estimated to reach US$221.65 billion in 2022 and approximately US$254.52 billion in 2023. It is also forecast to grow at an annual rate of 10.3% over the next few years, reaching US$505.5 billion by 2030 (Grand View Research, 2018–2021).

The third major area of impact of the Covid-19 pandemic on international food systems was agriculture and the food industry. Disruptions in supply chains due to numerous international and domestic transport restrictions worsened access to seeds, fertilisers and agricultural equipment, significantly affecting agricultural productivity worldwide. On the other hand, global container shortages and port congestion due to lockdowns and health restrictions have contributed to delays in the delivery of key agricultural commodities, increasing transport costs by up to 30% (Kuźmicz, 2022). The negative effects of the pandemic

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

particularly affected road transport, as the introduction of additional border controls and quarantine for truck drivers made it difficult to transport goods on both domestic and international routes (Dinçer *et al*., 2024).

Pandemic-induced global disruptions in demand and supply have led to volatility in the prices of many agricultural products. In 2020, wheat prices increased by 19% and rice prices by 12% (Polish Economic Institute, 2020), mainly due to export bans imposed by key exporters such as Russia and Vietnam. Farmers often had to sell their produce at lower prices due to oversupply or lack of markets. Many farms faced serious financial problems due to falling incomes and increased operating costs, including higher prices for seed, fertiliser and feed.

At the same time, the Covid-19 pandemic has forced farmers to adapt and change their farming practices. Many farms have begun to invest in technology, such as e-commerce and digital farm management tools, to better cope with the disruption. In China, for example, e-commerce platforms reported an increase of more than 100% in agricultural sales by 2020 (Guo *et al*., 2022). The pandemic has also highlighted the need for sustainable agriculture and local supply chains. Many farms have started to pay more attention to sustainable practices such as agroforestry, mixed cropping and local direct sales to increase their resilience to future crises. In Europe, a 15% increase in the number of farms using agroforestry was reported in 2021, contributing to increased biodiversity and improved soil quality (Mupepele *et al*., 2021).

The COVID-19 pandemic also had a significant impact on food processing plants around the world, leading to numerous disruptions in production, logistics and sales. Many food processing plants have been affected by massive worker infections, leading to temporary closures and reduced production, ultimately affecting their ability to maintain continuity of production and distribution. In addition, food producers had to adapt to increased sanitary requirements, which, with declining revenues, led to significant financial challenges including rising operating costs. In addition to having to invest in new safety measures, processors also had to cope with labour shortages and reduced production capacity. As with trade and agriculture, the Covid-19 pandemic

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

highlighted the need for greater flexibility and resilience in the food industry. Food processing plants have had to adapt quickly to new realities, investing in technology, changing operational practices and adapting to new sanitary requirements to ensure the future sustainability of food production and distribution (Soucheray, 2020).

CHALLENGES TO INTERNATIONAL FOOD SYSTEMS FROM THE COVID-19 PANDEMIC

The impact that the Covid-19 pandemic has had on international food systems has contributed to the identification of challenges in this area, which can be analysed along three key dimensions: food security, resilience of international food systems, and innovation and new technologies. However, it should not be forgotten that, in hindsight, the pandemic has also been a catalyst for positive change, forcing the agricultural and food sectors to adapt quickly to the new reality.

The biggest challenge the pandemic posed to international food systems was the increase in the number of undernourished and hungry people worldwide. According to a UN report, in 2020, the number of people affected by hunger increased by about 118 million, bringing the total number of hungry people worldwide to about 768 million (10% of the global population) (FAO, 2021). This increase was mainly due to disruptions in food supply chains, falling incomes and reduced access to food as a result of lockdowns and restrictions. The largest increase in hunger was in Africa, where about 21% of the population was malnourished. In Asia, the figure was 418 million people, accounting for more than half of the world's undernourished. In Latin America and the Caribbean, some 60 million people suffered from hunger (FAO, 2021). In response to the food crisis, many governments introduced support programmes to mitigate the effects of the pandemic. An example is the Paycheck Protection Program in the USA, which provided financial support to farmers and food producers (Economic Research Service, 2023). International organisations such as the Food and Agriculture Organisation – FAO, the World Food Programme – WFP, the

UN Children's Fund – UNICEF and the World Health Organisation – WHO have also taken steps to improve the food situation.

FAO implemented the Global Response and Recovery Plan, focusing on supporting smallholder farmers, improving food availability and strengthening food systems. As part of its implementation, it worked with governments and non-governmental partners to provide technical and financial support to the agricultural sector and continuity of agricultural production, particularly in African countries (FAO, 2020). WFP launched special transport flights and logistics operations to deliver food to hard-to-reach regions such as Yemen and South Sudan (WFP, 2020). UNICEF focused on providing food and nutritional support to children and families affected by the pandemic. The organisation provided therapeutic food, food parcels and supplements to children in countries, such as Ethiopia and Bangladesh, where access to food was particularly limited (UNICEF, 2023). The WHO also became actively involved to provide health and nutrition support to communities affected by the pandemic.

The drastic deterioration of global food security has triggered a wide-ranging discussion on the resilience of international food systems to international disruptions. Its main focus was on strategies to enhance their ability to cope with future crises, including the need to diversify sources of supply and create regional and local supply chains. Many experts also highlighted the need to simultaneously promote sustainable agricultural practices such as agroforestry, mixed farming or regenerative agriculture (Selvan *et al*., 2023). This is because they were considered importantin terms of increasing the resilience of food systems, improving biodiversity and soil health, as well as localising food production and supporting local markets, contributing to reducing dependence on international trade and increasing food security at regional level. Attention was also drawn to the need for coordinated action at international level, including financial support policies and programmes targeting farmers, promoting investment in infrastructure and the development of social security systems.

A key challenge, was also the issue of innovation and new technologies, considered an important element of the strategy to build the resilience of international food systems to future crises.

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Indeed, the experience of the pandemic showed that a flexible approach to new technologies and the ability to respond to emerging challenges were integral to the agri-food sector's adaptation to new circumstances.

Firstly, (as mentioned above), the COVID-19 pandemic forced the industry to rapidly move to digital sales channels, which was a challenge for both food manufacturers and retailers. Lockdowns and restrictions on movement ultimately caused a surge in demand for online shopping, which in turn required companies to invest in e-commerce, sales platforms and online payment technologies.

Secondly, disruptions in supply chains and limited availability of workers have forced companies to rapidly implement automation in production and logistics processes. Food processing companies have had to invest in technologies such as robotics, artificial intelligence (AI) and the Internet of Things (IoT) to reduce reliance on human labour and increase operational efficiency (Dadhaneeya *et al.*, 2023).

Thirdly, the need to ensure food safety and compliance with health regulations has increased the demand for tracking and transparency technologies in supply chains. Blockchain and other data logging technologies have therefore become crucial for tracking the origin of food products, monitoring transport conditions and managing risks in real time (Cao *et al.*, 2022).

Fourthly, the pandemic has also accelerated the adoption of precision farming technologies that allow for more efficient resource management and increased agricultural productivity. These technologies include the use of drones, sensors, data analytics and farm management systems that help farmers optimise irrigation, fertilisation and crop protection (Sridhar, 2023).

It can therefore be concluded that the Covid-19 pandemic has made a significant contribution to accelerating the adoption of technological innovations in the agricultural and food sectors, which have become crucial to maintaining the continuity of food production and distribution, but has also highlighted the need for further investment in new technologies that can increase the resilience of international food systems in the future.

PROSPECTS FOR INTERNATIONAL FOOD SYSTEMS IN THE LIGHT OF THE COVID-19 PANDEMIC EXPERIENCE

On the one hand, the Covid-19 pandemic has exposed many of the weaknesses of international food systems, while on the other, it has created new opportunities and directions for their development that can make them more resilient to future crises. One of the main lessons learned from the pandemic is the need to shorten existing supply chains and thus strengthen those of a local and regional nature. This is because there is no doubt that local supply chains are less dependent on international transport, making them less vulnerable to global disruption. Secondly, local and regional supply chains are better prepared for sudden changes in demand and supply, ensuring a more stable and predictable food supply. Indeed, shorter supply chains mean faster delivery of fresh food to consumers, which improves food quality and reduces losses, especially for perishable products such as fruit, vegetables and meat. Thirdly, strengthening local supply chains can contribute to the development of local farming and processing businesses, which can create new jobs and generate economic growth in agricultural regions. Fourthly, reducing long-distance transport, especially air transport, means reducing greenhouse gas emissions and is therefore an important instrument in the fight against climate change.

Tendencies to shorten supply chains have already emerged during pandemics. Examples include the Farmers to Families Food Box programme (US Department of Agriculture, 2024) in the US, which helped farmers sell their produce directly to consumers during a pandemic, or the European Union's 2020 Farm-to-Fork strategy (Milicevic & Nègre, 2023), whose goals and objectives make it an important step towards building more resilient and sustainable food systems by promoting local food production and consumption.

The experience of the pandemic also brought increased interest in food self-sufficiency policies. Many countries that experienced food supply problems chose to increase their foodself-sufficiency for pragmatic reasons – countries with greater self-sufficiency were less vulnerable to global food supply disruptions, giving them greater stability of supply and food availability even in

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

the face of crisis. A good example in this context is Singapore, which, as a small city-state, relies heavily on food imports. In response to the pandemic, Singapore has stepped up its efforts under the 'Singapore Food Story' programme, which aims to increase self-sufficiency in food production from 10% to 30% by 2030 (Singapore Food Agency, 2024). These efforts include the development of urban agriculture, aquaculture and innovative food technologies such as alternative proteins and precision agriculture. Another example is Qatar, which is one of the driest and hottest countries in the world. Indeed, in response to the pandemic, Qatar has stepped up its efforts in the area of domestic agricultural production, increasing funding for the development of agricultural technologies such as hydroponics and vertical farming, which has allowed it to increase production of vegetables and other agricultural products (Business Start Up Qatar, 2023). Interestingly, it has also managed to become self-sufficient in dairy production, a significant achievement given its previous dependence on imports (Islamic Organisation for Food Security, 2022).

The experience of the pandemic and its impact on international food systems also intensified calls for changes in agricultural and food policies both at the state and international levels. These were based on the weaknesses and risks revealed by the crisis, which were largely due to the limitations that characterised existing policies. In the case of countries, many have taken steps to, on the one hand, strengthen local food systems in order to become independent from international supply chains and, on the other, to promote sustainable agricultural practices in order to increase resilience to future crises. An example in this context can be seen in Germany and France, which have introduced new policies to support organic and regenerative agriculture – more resilient to climate change and other disruptions (Kurth *et al.*, 2023). In Germany, agricultural policy has focused on support for organic farming through subsidies and programmes to promote sustainable practices. France, on the other hand, has stepped up its 'Farm to Table Strategy', promoting regenerative agriculture and supporting initiatives to reduce pesticide use and improve soil health (Chivée & Mies, 2023). For countries reliant on food imports, the policy shift has primarily meant increased

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

diversification of supply. Such steps have been taken, for example, by Qatar, which has established new trade partnerships with Turkey and India, among others, allowing for greater stability of supply and reducing the risks associated with dependence on one or a few suppliers (Al-Abdelmalek *et al*., 2023).

The demands for changes in agricultural policy were not only limited to the level of countries, but also concerned the global level. Indeed, the experience of Covid-19 increased the emphasis on intensifying international cooperation particularly in the area of food security. Organisations such as FAO, WHO and WFP, for example, have taken a number of initiatives to better coordinate international action in support of the countries most affected by the food crisis. In response to disruptions in international trade, many countries and international organisations, including the World Trade Organisation, have advocated the need to accelerate international trade policy reform, including reducing trade barriers and improving the fluidity of food trade, emphasising the need to keep markets open and avoid protectionist policies that can disrupt global food supply chains. In response to the challenges of the pandemic, support to the least developed countries most vulnerable to the pandemic has also intensified. These efforts included financial assistance, technical assistance and the supply of food and other essential commodities to mitigate the impact of the food crisis.

SUMMARY

Summarising the above, it is important to note that, on the one hand, the Covid-19 pandemic exposed the fragility of international food systems and, on the other, their vulnerability to global disruptions and risks. The analysis conducted above also allows the following conclusions to be drawn. First, in view of the pandemic's impact discussed above, it is important to recognise that local and regional food systems are key to ensuring supply stability and food security. Indeed, investment in the development of local markets, logistics centres and storage infrastructure can reduce dependence on international supply chains and make food systems more resilient to global disruptions.

Secondly, sustainable agricultural practices, such as organic and regenerative agriculture, are essential for increasing the resilience of food systems to future crises. Implementing such practices not only improves soil health and increases biodiversity, but also contributes to the fight against climate change.

Thirdly, the implementation of new technologies, such as e-commerce, automation and tracking and transparency systems, are improving the efficiency and flexibility of food systems, helping to minimise the risks of disruption to global food chains.

Fourth, international cooperation and reforms of agricultural and food policies at the state and international levels are crucial to manage global food resources, ensure global food security and increase resilience to future crises, especially in the poorest countries and those dependent on food imports.

BIBLIOGRAPHY

Al-Abdelmalek, N., Kucukvar, M., C., Onat, N., Fares, E., Ayad, H., Bulak, M. E., Ekren, B. Y., Kazancoglu, Y., & Ertogral, K. (2023). Transforming Challenges into Opportunities for Qatar's Food Industry: Self-Sufficiency. *Sustainability*, *15*(7), Article 5755. https://doi.org/10.3390/su15075755

Business Start Up Quatar (2023, September 17). *Qatar successfully boosts security of essential food items*. https://www.businessstartupqatar.com/news/qatar-successfully-boosts-security-essential-food-items/

Cao, Y., Yi, Ch., Wan, G., Hu, H., Li, Q., & Wang, S. (2022). An analysis on the role of blockchain-based platforms in agricultural supply chains. *Transportation Research Part E: Logistics and Transportation Review*, *163*, 102–731. https://doi.org/10.1016/j.tre.2022.102731

Chivée, G., & Mies, A. (2023, October 23). *Effective regenerative agricultural practices in France: A farmer's perspective*. South Pole. https://www.southpole.com/blog/effective-regenerative-agricultural-practices-in-france-a-farmers-perspective

Dadhaneeya, H., Nema, P. K., & Arora, V. K. (2023). Internet of Things in food processing and its potential in Industry 4.0 era: A review. *Trends in Food Science & Technology*, *139*, 104–109. https://doi.org/10.1016/j.tifs.2023.07.006

Dinçer, F. C. Y., Ramazan, S., & Yirmibeşoğlu, G. (2024). A Qualitative Study on Covid-19 Effects on Logistics and Road Freight Transport:

The Case of Cold Chain Transportation Companies in Turkey. *Transport in Development Economics*, *10*, 13. https://doi.org/10.1007/s40890–024–00201–5

Dury, S., Alpha, A., Zakhia-Rozis, N., & Giordano, T. (2020). The COVID-19 crisis is challenging the food systems in Africa. *Cahiers Agricultures*, *30*. https://doi.org/10.1051/cagri/2020052

European Parliament (2023). *Field-to-table strategy*. https://www.europarl.europa.eu/factsheets/pl/sheet/293547/strategia-od-pola-do-stolu-

E-vegetables (2020, July 27). *Germany: lack of foreign workers has resulted in a smaller asparagus harvest*. https://www.e-warzywnictwo.pl/niemcy-brak-pracownikow-z-zagranicy-spowodowal-mniejsze-zbiory-szparagow,71,artykul,1,5542

FAO (n.d.). *Food systems and value chains: definitions and characteristics*. Climate Smart Agriculture Sourcebook, B10 – 2 Food systems and value chains: definitions and characteristics. Climate Smart Agriculture Sourcebook. Food and Agriculture Organization of the United Nations (fao.org).

FAO (2020). *Global Response and Recovery Plan*. https://openknowledge.fao.org/handle/20.500.14283/cb0439en

FAO (2021). *The State of Food Security and Nutrition in the World 2021*. https://openknowledge.fao.org/items/efd29e45–4004–4ec0-baad-eb9ea69278eb (28–07–2024).

Felix, I., Martin, A., Mehta, V., & Mueller, C. (2020, July 2). *US food supply chain: Disruptions and implications from COVID-19*. https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/us-food-supply-chain-disruptions-and-implications-from-covid-19 (26–07–2024).

Giri, A. K., Subedi, D., & Kassel, K. (2023, October 23). *Paycheck Protection Program loans provided $5.8 billion to U.S. farm sector in 2020*. US Department on Agriculture. https://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=107675

Grand View Research (2018–2021). *Online Food Delivery Market Size, Share & Trends Analysis Report By Type (Platform to Consumer, Restaurant to Consumer), By Region (North America, Europe), And Segment Forecasts, 2023–2030*. https://www.grandviewresearch.com/industry-analysis/online-food-delivery-market-report

Guo, J., Jin, S., Zhao, J., Wang, H., & Zhao, F. (2022). Has COVID-19 accelerated the E-commerce of agricultural products? Evidence from sales data of E-stores in China. *Food Policy*, *112*, Article 102377. https://doi.org/10.1016/j.foodpol.2022.102377

Islamic Organization for Food Security (2022, October 31). *How self-sufficient is Qatar in its food supply?* https://iofs.org/fr/post/979

Kowalska, A., Budzyńska, A., & Białowąs, T. (2022). Food export restrictions during the COVID-19 pandemic: Real and potential effects on food security *International Journal of Management and Economics*, *58*(4), 409–424. https://doi.org/10.2478/ijme-2022–0023

Kurth, T., Subei, B., Plötner, P., & Krämer, S. (2023, January 23). *Agribusiness Industry. The Case for Regenerative Agriculture in Germany and Beyond*. https://www.bcg.com/publications/2023/regenerative-agriculture-benefits-germany-beyond

Kuźmicz, K. A. (2022). Impact of the COVID-19 Pandemic Disruptions on Container Transport. *Engineering Management in Production and Services*, *14*(2), 106–115. https://doi.org/10.2478/emj-2022–0020

Mishra, A., Bruno, E., & Zilberman, D. (2021). Compound natural and human disasters: Managing drought and COVID-19 to sustain global agriculture and food sectors. *Science of The Total Environment*, *754*, Article 142210. https://doi.org/10.1016/j.scitotenv.2020.142210

Mupepele, A.-Ch., Keller, M., & Dormann, C. F. (2021). European agroforestry has no unequivocal effect on biodiversity: A time-cumulative meta-analysis. *BMC Ecology and Evolution*, *21*, Article 193. https://link.springer.com/article/10.1186/s12862–021–01911–9

Polish Economic Institute (2020, April 23). *PIE Economic Weekly*. https://pie.net.pl/wp-content/uploads/2020/04/Tygodnik-Gospodarczy-PIE_16–2020.pdf

Selvan, T., Panmei, L., Murasing, K. K., Guleria, V., Ramesh, K. R., Bhardwaj, D. R., Thakur, C. L., Kumar, D., Sharma, P., Umedsinh, R. D., Kayalvizhi, D., & Deshmukh, H. K. (2023). Circular economy in agriculture: Unleashing the potential of integrated organic farming for food security and sustainable development. *Frontiers in Sustainable Food Systems*, 7. https://doi.org/10.3389/fsufs.2023.1170380

Singapore Food Agency (n.d.). *Our Singapore Food Story*. https://www.sfa.gov.sg/fromSGtoSG/our-sg-food-story (26–07–2024).

Soucheray, S. (2020, April 27). *US food processing plants become COVID-19 hot spots*. CIDRAP News. https://www.cidrap.umn.edu/covid-19/us-food-processing-plants-become-covid-19-hot-spots

Sparrow, J. (2020, March 4). *COVID-19: Managing supply chain risk areas. How traditional models will change*. https://www.deloitte.com/global/en/services/risk-advisory/analysis/covid-19-managing-supply-chain-risk-and-disruption.html

Sridhar, A., Balakrishnan, A., Jacob, M. M., Sillanpää, M., & Dayanandan, N. (2023). Global impact of COVID-19 on agriculture: Role of sustainable agriculture and digital farming. *Environmental*

Science and Pollution Research, 30, 42509–42525. https://doi.org/10.1007/s11356–022–19358-w Taleb, N. N. (2007). *Black Swan. How unpredictable events rule our lives*. Random House.

UNICEF (2023, May). *Ready-to-Use Therapeutic Food: Market and Supply, Update, May 2023*. https://www.unicef.org/supply/media/17331/file/Ready-to-Use-Therapeutic-Food-Market-and-Supply-Update-May-2023.pdf

US Department of Agriculture (n.d.). *USDA Farmers to Families Food Box*. https://www.ams.usda.gov/selling-food-to-usda/farmers-to-families-food-box

WFP (2020, December 20). *External Situation Report, Covid – 19, No 10*. https://www.wfp.org/publications/covid-19-situation-reports

World Economic Forum (2020, April 7). *U.S. dairy farmers dump milk as pandemic upends food markets*. https://www.weforum.org/agenda/2020/04/dairy-milk-pandemic-supply-chains-coronavirus-covid19-pandemic/

Zhou, J., & Delgado, C. (2020, June 26). *The impact of COVID-19 on critical global food supply chains and food security*. Stockholm International Peace Research Institute. https://www.sipri.org/commentary/topical-backgrounder/2020/impact-covid-19-critical-global-food-supply-chains-and-food-security

Marzęda-Młynarska, K. (2025). Challenges and prospects for international food systems in the light of the Covid-19 pandemic experience. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 59–74). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Justyna Szulich-Kałuża

Faculty of Social Sciences of the John Paul II Catholic University of Lublin, Institute of Journalism and Management
E-mail: justyna.szulich-kaluza@kul.pl
ORCID: 0000-0002-6845-168X

Małgorzata Sławek-Czochra

Faculty of Social Sciences of the John Paul II Catholic University of Lublin, Institute of Journalism and Management
E-mail: malgorzata.slawek-czochra@kul.pl
ORCID: 0000-0002-4732-1341

COVID PASSPORTS IN POLAND AND EUROPE – SYMPTOM OF POST-PANDEMIC NORMALISATION OR BEHAVIOURAL INTERVENTION? A STUDY BASED ON EMPIRICAL RESEARCH AND DISCOURSE ANALYSIS

Abstract: The aim of the article was to determine whether COVID passports were perceived by citizens of Poland and other EU countries as an effective tool leading to post-pandemic normalisation or as a behavioural intervention to bring about a change in citizens' behaviour. Due to the complexity of the research problem, it was decided to use a diversification of materials as well as research methods. A secondary quantitative and qualitative content analysis of the *Eurobarometer* reports *Public opinion monitoring in the time of COVID-19: Europeans' reactions and perceptions of the COVID-19 pandemic* and a discourse analysis of media material from Internet resources in terms of perceptions/opinions about COVID passports were carried out. A main thesis was put forward, stating that COVID passports were primarily an instrument of behavioural intervention to encourage

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

vaccination uptake, leading to far-reaching social change, and three derived specific hypotheses: H.1. The results of the self-analyses indicate that the outcome of the behavioural intervention was the practice of perceiving COVID passports as a pass to the normality of social life (incentive – tourism, events, shops and restaurants); H.2. The results of the self-analyses indicate that the outcome of the behavioural intervention was the practice of perceiving COVID passports as digital surveillance tools leading to loss of personal freedom; H.3. The results of the self-analyses indicate that the outcome of the behavioural intervention was the practice of discrimination against unvaccinated people framed as a punishment for avoiding vaccination. All hypotheses were positively verified through interpretation and inductive inference.

Keywords: COVID passports, public behavioural intervention, COVID-19, post-pandemic reality, Poland, European Union.

INTRODUCTION

The World Health Organisation on 11 March 2020 declared COVID-19 a global pandemic. And while humanity had already struggled in the 21st century with the H1N1 influenza virus (2009–2010), SARS (2002–2004), MERS (2012), and Ebola (2014–2016), the emergence of the COVID-19 pandemic triggered action at a pace and scale that was new and surprising to citizens around the world (Bell, 2021, p. 60). The way in which the SARS-CoV-2 pandemic was handled highlighted the gap between the power of the United States, Europe, China and Russia and the global south, which was unable to develop its own solutions (Balfour *et al.*, 2022, pp. 3–4).

As part of international solidarity, the European Union has developed externally an initiative known as Team Europe. Internally, however, Member States have entrusted the European Commission with unprecedented tasks such as the purchase and distribution of vaccines. On 27 March 2021. The European Commission also presented its proposal to make credible COVID-19 vaccination certificates a reality in order to facilitate free movement during the COVID-19 pandemic (Narozniak & Princ, 2022, p. 34).

The EU COVID Certificate (UCC), vaccination passport or green pass are different terms for a document that was issued from 1 July 2021 and recognised by all 27 EU Member States and some non-EU countries. The document was intended to facilitate travel between the various EU countries and also allowed the use of public places, i.e. restaurants, galleries or cinemas, where limits on people being in an enclosed space had been introduced. By presenting this document, it was possible, among other things, to avoid quarantine upon arrival in a given country, although the exact mechanisms for this depended on the internal regulations of individual EU countries. The content of the certificate was written in both English and the national language. The certificate consisted of a QR code, which could be displayed on a mobile device or printed out, and a digital signature, verified through the EU Gateway to confirm a traveller's status in the context of possibly being a carrier of the SARS-CoV-2 coronavirus. The EU Certificates were proof that a person had been vaccinated against COVID-19, had tested negative for the coronavirus or was a recovering patient. It was originally intended to be valid for one year, but on 13 June 2022 its validity was extended for a further year – until 30 June 2023 (European Commission, 2022). Finally, it ceased to be required on 1 July 2023.

This article attempts to determine whether COVID passports were seen as an effective tool leading to post-pandemic normalisation or rather as a behavioural intervention to bring about a change in citizens' behaviour.

The new approach is called behavioural public interventions (BIPs). It has been developed in recent years by administrations in the United States, the United Kingdom, Denmark, the Netherlands or France (Lunn, 2014, pp. 25–38). The growing popularity of the application of the behavioural approach is a manifestation of a paradigmatic shift in the thinking and implementation of public actions, which may also be important for Poland and Poles. The preparation of so-called behavioural interventions, i.e. initiatives that use the insights of behavioural economics to change people's behaviour to benefit welfare and social order (Datta & Mullainathan, 2012; Shafir, 2013, p. 1), consists of four steps: defining the behaviour to be changed, identifying barriers to behaviour change, identifying behavioural tools for behaviour change, preparing an initiative that uses as many of these tools as possible and addressing as many barriers

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

as possible. Although public interventions can address a wide range of different aspects of citizens' lives they are based on a relatively simple logic of influencing citizens, which Bemelmans-Videc (2007) reduces to a division between 'carrots, sticks and preaching'. Interventions are thus based on punishments and bans, positive incentives or information and awareness raising (Olejniczak & Śliwowski, 2014, p. 15). Past experience suggests that the effectiveness of interventions depends on understanding the mechanisms of people's behaviour and how they make decisions (Shafir, 2013, p. 1). In other words, the interventions undertaken by public authorities will be more successful the better the intervention developers adapt their form and logic to the ways in which citizens make decisions. The behavioural approach rarely relies on education, as it is not an effective tool for behaviour change. Better results can be achieved by developing interventions to change the outcome of cost-benefit analysis, redesigning the context in which a decision is made or using the social context. The currently dominant public policy paradigm and the design of behavioural interventions assume that people are rational, driven by self-interest and seek to maximise their benefits while minimising their costs (Amadae, 2007), namely, they are largely selfish and will respond to incentives or prohibitions in a rational, thoughtful manner, calculating their gains and losses and considering all the 'pros and cons' (Low, 2011, pp. 1–2).

We therefore pose the following central question:

Do the analyses of empirical findings and multimodal discourse on COVID passports indicate practices that fit into the category of top-down designed behavioural intervention?

As well as specific research questions:

1. In the research material, are COVID passports seen as a document that puts the holder in a privileged position (carrot – a system of extended incentives – from returning to tourism through mass events to going out to restaurants)?
2. In the research material, are COVID passports seen as a tool for surveillance (e.g. biometric, behavioural) conducted using new technologies, and concerns about misuse of personal data?
3. Is the research material COVID passports are seen in terms of loss or punishment and there are opinions about

the loss of privacy and civil liberties in the context of the introduction of PC?

In this article, we hypothesise that COVID passports were primarily an instrument of behavioural intervention to encourage vaccination uptake, leading to far-reaching social change and derived directional hypotheses:

H.1. The results of the self-analyses indicate that the behavioural intervention resulted in the practice of perceiving COVID passports as a pass to the normality of social life (tourism, events, shops and restaurants).

H.2. The results of the self-analyses indicate that the outcome of the behavioural intervention was the practice of perceiving COVID passports as digital surveillance tools leading to a loss of personal freedom.

H.3. The results of our own analyses indicate that the outcome of the behavioural intervention was a practice of discrimination against the unvaccinated framed as a penalty for avoiding vaccination.

MATERIALS AND METHOD

Due to the complexity of the research problem, it was decided to use a diversification of materials as well as research methods. The research material in this study consists of available empirical research on perceptions of the COVID-19 pandemic in EU countries with a particular focus on opinions on COVID passports in Poland and other EU countries, as well as media materials from Internet resources in the form of publications on green passes.

The content analysis (Berelson, 1952, p. 8; Holsti, 1969; Krippendorff, 2004, p. 413; Neuendorf, 2017, p. 17) of the empirical findings included 24 reports of the Eurobarometer Monitoring Public Opinion at the Time of COVID-19, available in the European Parliament's online archives, containing data collected from 28 European countries including Poland for the period from March 2020 to June 2021, i.e. three waves of the pandemic.

In total, the reports include 764 opinions on the concerns and experienced consequences of the COVID-19 pandemic in both the health, economic and social fields. The largest

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

number of opinions were collected in Italy (79), Germany (72), Spain (61), the Czech Republic (60) and France (54), while the smallest number were collected in Luxembourg and Croatia (1 each). Poland is ranked 15th among the countries asked for opinions (22) (EP, 2020a, 2020b, 2020c, 2020d, 2020e, 2020f, 2020g, 2020h, 2020i, 2020j, 2020k, 2020l, 2020ł, 2020m, 2020n, 2020o, 2020p, 2020r, 2020s, 2021a, 2021b, 2021c, 2021d, 2021e, 2021f). This is interesting because in the vast majority of European countries, the number of reported pandemic impacts by the population of each country, corresponds to its position in the Worldometer's COVID-19 data, conditional on the number of recorded infections and deaths. The exceptions are the UK, whose exodus started even before it actually left EU structures, and Poland (Worldometer, 2020, 2021, 2022).

In general, the first questions about COVID passports arose in the second wave of the pandemic (FR, NL) between August and February 2021, when work on the vaccine was already well advanced and the first December vaccination events (EP, 2020n, 2020o, 2020p, 2020r, 2020s, 2021a, 2021b) had occurred. Opinions on COVID passports (36) represent 4.7% of all opinions on the fears and experienced consequences of the COVID-19 pandemic (764), and 16.2% of all opinions on its social impact (222).

Opinions of Polish citizens on COVID passports were not included until May during the third wave of the pandemic (March-June 2021) (EP, 2021c) and accounted for 2.7% of all opinions on COVID passports (EP, 2020n, 2020o, 2020p, 2020r, 2020s, 2021a, 2021b, 2021c, 2021d).

The number of opinions on COVID passports of EU residents, like the overall number of opinions on the pandemic, corresponds to the number of infections and deaths (Worldometer, 2020, 2021), with 13 out of 27 EU countries expressing it. The opinion was expressed by 3 (NL, SE, PT) out of 6 countries enthusiastic about vaccination (DK, FI, IE, MT, NL, PT, SE), 6 (BE, IT, ES, DE, FR, GR) out of 12 realistic (AT, BE, DE, EE, ES, FR, GR, IT, LT, LU, RO, SI) and 4 (PL, HU, LV, BG) out of 8 countries sceptical about vaccination (BG, CY, CZ, HR, HU, LV, PL, SK). A proportional selection criterion based on the attitudes towards vaccination of the citizens of each EU country was therefore applied.

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Public opinion polls conducted in the heat of the moment, in a crisis situation, are a valuable source of knowledge, allowing the authorities to continuously diagnose and choose the direction of change. Also of interest is the public's familiarity with the new document and its perception at a slightly later stage, which is to be served by discourse analysis of media materials.

Nowadays, it comes in different varieties – most often with the denominations critical analysis, linguistic analysis, social analysis (Kopytkowska & Kumiega, 2017, p. 177), and multimodal discourse analysis, which involves the study and interpretation of multiple codes used in a given communication, has been particularly popular in recent years. Multimodality is an interdisciplinary approach that provides concepts, methods and analytical frameworks for describing media practices with respect to their semiotic complexity. Multimodal and online communication increasingly model discursive practices (Bucher, 2015, p. 201).

The research task here is to identify the central discourse concepts (textual and visual) and their fillings (doxologies) that collectively construct social knowledge of COVID passports. This knowledge will be described using the assumptions of social representation theory, derived from Serge Moscovici (1984a, 1984b, 1988, 2000, 2001). We exploit the property of social representations specifying collective meaning-making processes, resulting in shared cognitive constructs that can change individual and collective thinking in society (Höijer, 2011, p. 3).

According to Moscovici (1984b, pp. 7–10), there are two main functions of representations. First, they conventionalise (anchor) concepts, persons, events and situations by giving them a concrete linguistic or visual form. They thus assign them to a general, previously known category, gradually isolating their common meanings.

Secondly, they are prescriptive in the sense that they are suggested to us and even imposed on us through social interactions, perpetuated structures and existing rules of social coexistence. Representations aim to "make something unfamiliar or the unfamiliarity itself familiar" (Moscovici, 1984b, p. 24). A number of mechanisms of conventionalisation of phenomena are used for this purpose, including: naming, emotional anchoring, thematic anchoring, metaphorical anchoring and anchoring by way of basic antinomies. Media representations will be treated as constructs that generate meanings and social knowledge of COVID passports.

When selecting the research corpus for the multimodal discourse analysis, it was decided to choose web texts using tools in the resources of Google, the most popular search engine among Internet users (https://www.google.com). According to Polish rankings, it ranks first and accounts for 93.86% of all search traffic and queries of Internet users on the web (Mediapanel, 2023). Using the keywords*: COVID passports* in a year, we obtained a list of 100 items ordered according to the relevance of the search engine's recommendation algorithm (date of material selection and selection: 25 April 2023). An important element of the Internet user's activity is the use of references/links in the web structure and the individual composition of thematically related hypertexts. Aiming to faithfully emulate the Internet user environment, we indexed the network of related texts to two levels of depth. Accordingly, our dataset contained an item list of 100 consecutive, non-repeating natural search results (organic search – free links to websites) from the first search and algorithmically selected material from the second depth level for the items in the first list. Then, guided by purposive selection, a set of texts was selected for the final analysis, which substantively corresponded most closely to the subject of the study. The units of analysis were whole texts, together with their layout and visual elements. The final catalogue included digital publications from the following domains: www.gazetaprawna.pl (26), www.rp.pl (11), www.fakt.pl (3), www.wiadomości.wp.pl (3), www.krytykapolityczna.pl (2).

RESULTS AND DISCUSSION

1. COVID PASSPORTS IN EUROPEAN UNION SURVEYS

1.1. COVID passports as proof of security and document for returning to normality

Positive opinions on the introduction of vaccination passports clearly resounded in the survey material analysed. Citizens from

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

11 EU Member States including Poland expressed 21 opinions (BEx2, ITx4, PTx3, ESx3, DEx2, SE, FRx2, NL, PL, HU, LV) indicating the following positives:

- the possibility of renewed free movement within the EU (13 opinions);
- participation in public cultural and sporting events (12 opinions);
- security in shops, restaurants and offices (9 opinions);
- encouraging vaccination (3 opinions).

Overall, EU citizens agree that the COVID passport is an effective tool and will provide security when travelling and in larger gatherings of people, but there is no clear support for this solution (EP, 2021c). 76% of Italian adults are convinced of its effectiveness, 75% of Spaniards, but only 57% of Poles and 52% of Hungarians. Only 21% of Poles strongly agree that it will be an effective tool in the fight against a pandemic and will ensure the safety of travel and major events; 36% tend to agree, 15 tend to disagree, 18% strongly disagree and 9% are not sure (EP, 2021c). The introduction of EU COVID Certificates is more likely to be supported by older respondents, aged 55 or over (71%–73% depending on the category), residents of the largest cities (72%) and respondents from households with an income of at least PLN 3,000 per capita (75%) (EP, 2021c; Omyła-Rudzka, 2021, p. 7).

Its effectiveness is slightly more believed in by women 73% than men 72%, those between 50 and 74 years 76% to 70% under 35 years, with higher education 75% to 70% with lower education (EP, 2021e). The results of the analysis corroborate the findings of studies showing a correlation between age, gender, education and income and attitudes from COVID passports conducted in the USA, UK and Japan (Garrett *et al.*, 2021; Drury *et.al.*, 2021).

Only just over half (58%) of Poles believe that a COVID passport should be required for entry into the country while Italians (79%) or Spaniards (77%) see it as a necessary security measure. Only 27% of adult Poles strongly agree, 32% tend to agree, 15% tend to disagree, 17% strongly disagree and 10% are not sure.

Only 49% of Polish citizens see its usefulness as security for mass events and even fewer (36%) think it should be required in shops, restaurants or offices.

Only 22% of Polish adults think that all large public venues such as concert halls and stadiums should require a vaccine passport, 27% rather should, 20% rather disagree, 22% strongly disagree, 9% are not sure.

As many as 27% of Poles strongly disagree that the document should be required in shops, catering establishments and offices, 28% tend to disagree, 22% tend to agree and 14% strongly agree, 10% have no opinion (EP, 2021c). The quoted results indicate that Poles, in contrast to many other nations, do not see the need to monitor their activity within their own country, believing it to be too much of a cost, leading to digital monitoring of citizens' behaviour, which was done by means of mobile applications and activity analysis by means of developed online algorithms. This supports hypothesis 2, stating that the result of the behavioural intervention was the practice of seeing COVID passports as digital surveillance tools leading to a loss of personal freedom.

The results of the analysis also indicate that Poles, like many other EU residents, perceive the personal benefits of having a vaccination passport (34 opinions) and the fact that they can motivate people to receive the vaccine (3), in line with results also obtained outside the European Union in the USA, UK and Japan (Garrett *et al*., 2021). The data obtained from the analysis of the reports allow us to positively verify hypothesis one, stating that the outcome of the behavioural intervention was the practice of perceiving COVID passports as a pass to normal social life (tourism, events, shops and restaurants).

Ultimately, the analyses show that attitudes to the introduction of certificates make the biggest difference in respondents' attitudes to vaccination. Respondents who have already vaccinated with at least one dose are 80% in favour of COVID passports, as are respondents who definitely want to vaccinate (73%) and would rather take the vaccine (71%). In contrast, those who definitely do not intend to vaccinate and are unlikely to take the vaccine are mostly opposed by 80% and 66% respectively (Omyła-Rudzka, 2021, p. 7). This shows that the strongest inhibitor or obstacle to be eliminated was the fear of taking the vaccine. The cited results confirm the positive relationship between vaccination and attitudes towards passports described in a similar study conducted in the UK (de Figueiredo *et al*., 2021).

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

1.2. The COVID passport as a source of concern, controversy and risks

The analysis of the survey material showed that Poles and citizens from other 8 EU Member States expressed 15 opinions (DEx3, PTx2, ESx2, FRx2, BE, IT, BG, NL, PL) indicating the following negatives of the introduction of COVID passports:

- may lead to discrimination against non-vaccinated persons (10 opinions),
- threatens patient's confidential medical data – government/employer/private app providers will receive it along with vaccination information – (9 views),
- will bring negative consequences for business (2 opinions),
- can lead to discrimination against the poor (free screening for people who have not had the opportunity to be vaccinated (2 opinions),
- the dangers of reintroducing free travel and tourism (2 opinions).

The results signal the existence of discriminatory mechanisms hidden in the introduction of PC, which place unvaccinated persons in an exclusionary situation (e.g. for health, religious, economic or institutional reasons), indicating the existence of an incentive (normal social life) as well as a penalty (exclusion from social life) for avoiding vaccination. Nevertheless, it is evident that Poles, as well as other inhabitants, when weighing all the "pros and cons", point to ethical, legal, political and moral doubts that arise here. The data obtained allow us to positively verify the third hypothesis, which states that the behavioural intervention resulted in the practice of discrimination against non-vaccinated persons.

Adult, employed Poles are particularly concerned about revealing their personal data and information about their health status to their employer (55%), government institutions (63%) and private application companies (66%). As many as 72% trust their doctors and are comfortable with the knowledge that they have access to information about their health status and vaccinations received.

Overall among the Europeans surveyed, younger people (under 35) feel more comfortable allowing their employer (57%), government (52%) and private companies (45%) access to their personal health information than older people (50 to 74), (54%,

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

47%, 33%). Those with higher levels of education are slightly more satisfied that their employer (58%), government (54%) and private companies (44%) have access to their health information than those with lower levels of education (55%, 46%, 38%). The results of the analysis clearly indicate concerns about personal security and the annihilation of the private sphere as a result of COVID-19 restrictions (Momani, 2020). Respondents fear the loss of control over their digital identity of data collection and algorithmic analysis of individuals, which Alexei Krivolap (2022) writes about when showing the world of the glass man with nothing to hide, confirming hypothesis two.

2. CENTRAL LINGUISTIC CONCEPTS OF COVID DISCOURSE

2.1. COVID passports – history of the idea, objectives and rules of application

The linguistic expressions of the analysed hypertext form definitional scripts about COVID passports, exposing content about enabling access to tourist activities, cultural activities and amenities in daily life:

> Digital Green Certificate [...] used not only to facilitate free travel but also as a ticket to events (PC-6), mild coercion, i.e. sanitary passports (PC-17); common EU immunity certificates, standardised vaccine passports, an app with a unique QR code containing personal data and information on being vaccinated, a special app being developed in cooperation with the intelligence community to be ready for download (PC-2), a digital document (also to work as an app on a smartphone), a digital pass that should make life easier for Europeans (PC-4).

COVID passports require an international consensus, defining detailed technical specifications, as to the format of the certificates, specifically:

> A supranational agreement on a common certificate without which safe travel cannot be restored (PC-2); the EC chief expressed the view that passports should be based on elements such as vaccination

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

> information, a negative test result for SARS-CoV-2 or the acquisition of immunity after COVID-19. She estimated that it would take about three months to implement the vaccination certificate system (PC-3).

In the publications analysed, we find indications of the intentionality of the passports in the direct statements of the experts to signal the authenticity and scientific objectivity of the discourse:

> The aim of the passports is not only to keep the population safe from people spreading the virus but also to get them to be vaccinated. "Vaccine passports can be used as an incentive to change behaviour. [...] They signal what society expects of individuals. They express a social norm to which people should conform. They are no different from other forms of conditioning used in many settings / Dr Joan Costa-Font, health economist at the London School of Economics" (PC-6).

The introduction of passports is intended to prevent an uncoordinated, open and flexible approach by individual countries to these documents:

> The Brussels initiative is an attempt to stop a repeat of the chaos in movement across the EU that prevailed before the introduction of the COVID-19 certificate. [...] the worsening epidemiological situation poses the risk of differing approaches by countries to this document. France has already announced that the certificate for those not vaccinated with the booster dose will expire on 15 January 2022. In addition, the validity of the tests, which were supposed to be an alternative to vaccination, will be limited to 24 hours in France (initially it was 72 hours, then 48 hours). This is precisely the situation of different treatment of the certificate that we want to avoid (PC-9).

2.2. COVID passports as privileged proof of security, return to normality, access to tourism and cultural and social life, economic development

This central notion is filled with content about COVID passports in a display of positives. Quoted statements from politicians,

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

government officials and EU representatives reinforce the thematic anchoring relating to the advantages and benefits of the certificates:

> COVID passports is the idea of a common EU immunity certificate that unites tourism countries. These include, in particular, countries where tourism is (or rather was) one of the most profitable industries (PC-2); […] COVID passports, testing on a massive scale, introducing privileges for those who are vaccinated, and finally compulsory vaccination […]. These are safety standards that have worked and are working in many countries so that today they are just loosening the restrictions (PC-13).

Linguistic expressions compile positive associations of passports with economic development, effectiveness of vaccine promotion and control of vaccine campaigns:

> Certificates in Europe have proven to be the best means of promoting vaccination (PC-12); People must finally be made aware of the fact that vaccination is a gift, not a compulsion! Of course you don't have to be vaccinated if you don't want to go to the theatre or the cinema (PC-18); 'Green passports' will boost the economy and encourage vaccination sceptics […] countries that are introducing similar solutions hope that e-certificates will, in time, become a convenience for travellers […] health 'passports' for the time being can only be useful from a medical point of view as a tool to improve surveillance of vaccination campaigns and recorded side effects. […] Such a solution would allow certain groups to reasonably return to normal functioning in society. Various forms of 'rewards' could also become an incentive to vaccinate for those who have so far been hesitant: you show social solidarity, you gain immunity, and on top of that you can do more; if you don't show solidarity, you suffer the consequences (PC-5); More vaccinated, fewer deaths and hospitalisations, and less loss to GDP – these are the effects of the introduction of the COVID passport. […] Thus, Bruegel analysts estimate that the passports avoided in the second half of 2021 a GDP loss of €6 billion in France, €1.4 billion in Germany and €2.1 billion in Italy. (PC-12); COVID passports would thus become passports to normality, once free and freely available, now rationed for public health reasons (PC-6).

The above discourse analyses allow us to confirm hypotheses one, two and three by linking COVID passports to a system of incentives, digital surveillance as well as consequences (penalties) related to vaccination avoidance.

2.3. COVID passports as evidence of behavioural interventions, a source of concern, controversy and risk

The next central notion can be described as a multi-vocal statement about COVID passports in the exposure of negatives. Here we find statements about the controversies, concerns and doubts that the certificates raised:

> Possible vaccination passports would raise unparalleled objections in the United Kingdom [...]. In Finland, press comments stress that at this stage – when only about 5 per cent of the population has been vaccinated and international standards have not been developed – it is difficult to assume that certificates would provide benefits for travel, for example. Similar doubts are raised about the passport condition for admission to cultural or other mass events. There are claims from organisers that this would constitute a form of 'covert coercion to vaccinate'. On the other hand, attention is drawn to the fact that the audience for such events consists mainly of representatives of the younger generation, who are not likely to be vaccinated any time soon (PC-3): [...] here there is a kind of veil of silence in the European Union, i.e. we have no clear declarations as to what will happen next with passports (PC-10).

In response to the COVID-19 pandemic, many countries have introduced new methods of monitoring and surveillance of citizens using technological advances for these purposes, and this in turn can be seen as a threat to freedom and civil liberties. Some media statements touch on these issues and are particularly loaded, not least because of their strong emotional anchoring. These include statements by academic authorities, celebrities and politicians about unethicality, violations of privacy and personal freedoms, and contradictions with the rules of democracy, especially in the context of extending surveillance

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

and control over citizens along the lines of the behavioural interventions already used by European governments:

> COVID passports are proof that behavioural interventions targeted by governments at citizens should be banned. They are not only unethical, but also contrary to the rules of democracy. Behavioural manipulation has been used increasingly in public policy for at least two decades, ever since psychologists and behavioural economists such as Daniel Kahneman, Amos Tversky and later Richard Thaler and Cass Sunstein (with the exception of Sunstein, all Nobel laureates) described ways to influence people using knowledge of their cognitive biases. Considering such interventions as a standard policy tool pushes us into the arms of a soft, paternalistic totalitarianism. In such a regime, we may be left formally free to choose, but a caring authority ensures that we always choose what it expects of us (PC-6). This is everyone's decision [...]. It is about freedom. You are enslaved from all sides today. Even those f*** COVID passports. This selection is enslavement. It's not about persuading you to vaccinate. It's about holding people accountable whether they are vaccinated or not. Social accountability is something very important. However, we live in an age where free will is very much taken care of, so any attempt to coerce people to do anything will always be met with opposition. I am not saying whether it is good to be vaccinated or bad (PC-14); the exercise of fundamental freedoms is conditional on showing the appropriate certificate. In addition, this certificate depends on the acceptance of a second dose of a vaccine, about whose efficacy and safety there is often still some controversy. A vaccine that has not yet been fully tested in a proper, clinical manner. [...] We are against mandatory vaccination, and against the introduction of a vaccination certificate. For this is a blatant violation of fundamental freedoms (PC-15); Trouble with the COVID passport system has been reported by people who have chosen to be vaccinated with the Johnson & Johnson single-dose vaccine. After the system started to suspend their EU COVID certificates, the Ministry of Health stopped issuing them. For many citizens, however, this means a problem. They have business trips to England, Switzerland or Austria ahead of them, and their passports are no longer valid for a fortnight after receiving the booster dose (PC-7).

This helps confirm the veracity of hypothesis two stating that the result of the behavioural intervention was the practice of perceiving COVID passports as digital surveillance tools leading to a loss of personal freedom.

In addition, the central notion discussed is embedded in the discrimination against the unvaccinated and those without COVID passports. Exclusionary selection, however, has a second bottom – intervention and deliberate influence on specific social choices, which points to the truth of hypothesis three. It is also incompatible with respect for human freedom and may consequently hinder the building of trust in political and medical authorities:

> It is interesting that those reluctant to embrace the idea of a COVID passport often criticise it as unfair discrimination on the basis of belief or a Bill Gates conspiracy. They are unaware that it is in fact a tool to influence their attitudes and choices. What they are protesting against is not meant to punish them. It is supposed to change them. […] COVID passports are meant to condition perverse individuals by imposing costs on those of their choices that the authorities do not accept (PC-6).

The positive (practical) value of passports (reward) is juxtaposed with the restrictions imposed on the unvaccinated and their exclusion from participation in cultural, social, civic and economic activities (punishment). The expressions filling the central concepts clearly reinforce the unjust and discriminatory nature of passports from ethical, political, legal and scientific perspectives:

> For vaccine passports to be fair, everyone should have the chance to be vaccinated without incurring more costs, otherwise they will become potentially discriminatory. Firstly, some people will have to be excluded because they cannot be vaccinated due to allergies or pregnancy. Secondly, the immediate implementation of passports would prevent people in many lower-income countries from travelling, as they may not receive the vaccine until 2022 (PC-6); […] if vaccination is not mandatory, passports allowing travel would be discriminatory. […] the introduction of passes would discriminate

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

> against people who cannot yet be vaccinated because, for example, they do not belong to a risk group. In the Czech Republic, voices in favour of the introduction of passports were raised in January, when vaccination started and expectations were much higher than now. In the discussion, attention was drawn to the possibility of discrimination against certain groups of the population (PC-3); all because the governments in Paris and Berlin fear potential discrimination against unvaccinated Europeans. This is mainly about young people who do not belong to the priority groups and will mostly not be vaccinated until the holidays (PC-4).

3. VISUAL REPRESENTATIONS OF COVID PASSPORTS

The sample of materials taken from the pages allows us to assess visual representations as a constitutive element of multimodal discourse. The choice of images and illustrations remains with the senders and authors, who, by selecting them into specific textual formats, reproduce and shape, or even impose, specific social meanings. Visual codes in combination with linguistic ones lead to a multimodal construction of specific knowledge about COVID passports. The lines of visual discourse can be organised into three dominant visual representations. The first visualises the use of modern technology in the ways in which COVID passports are used and fits into the concept of a new biometric human identity, which supports hypothesis two. The identity indicated is based on biological data, such as fingerprints or a digital photograph, and has the hallmarks of a 'depersonalised' human identity. Such a 'personless' identity can easily lead to people being avoided, stigmatised and consequently excluded from the community (Ferdek, 2022, p. 57). Two further representations are visualisations of the dissemination and promotion of immunisation and the evocation of positive associations with passports. These are focused on the freedom to travel and it certainly represents dominant information with high positive associative power, confirming hypothesis one.

In the analysed corpus of online texts, the image has two functions: illustrative (the image serves the text – a hierarchical relationship) or complementary (text and image are semiotic partners – a linear relationship). Graphic highlights and illustrations evoke non-linear reception by navigating users to the exposed parts of the texts. We conclude that the process of reception and assimilation of images is controlled by conspicuous elements (salience theory) (Itti & Koch, 2000). The photographs and illustrations accompanying the texts are not numerous or varied. It can be inferred that the authors are drawing from a limited and versatile 'COVID' collection of photographs, graphics and illustrations, which is most likely a free online image bank. These are images deliberately designed for use in different contexts and do not necessarily faithfully record or document reality. The most numerous visual representation of COVID passports are illustrations of the QR code displayed on mobile phone displays. In general, the layout of visual materials is characterised by low sensory stimulation and poor interactivity in terms of stimulating the viewer's cognitive activity. It has to do with an unstructured hypertext structure, linearity and unidirectionality of communication, lack of selection and integration of different fragments of both texts and images. The authors selected visual codes that had the potential to become discursive dominant codes (e.g. QR codes of certificates on phone screens) – on the assumption that they would become codes illustrating current important communicative events and social situations, becoming part of the creation of desired meanings. The second group of codes will be called arbitrary (e.g. the symbolism of certificates as travel passports guaranteeing freedom of travel), i.e. universal, equally understood and read regardless of cultural conventions. In the research material it is possible to find, not entirely successful and well thought out, unrealistic representations associated with certificates. These deviate from natural reality and, according to the theory of social semiotics, representations that are not faithful representations of the natural world may be perceived as less credible (e.g. hyperbolisation of the vaccine ampoule and miniature people).

The graphical structure of the texts makes use of uncomplicated and unsophisticated measures: highlighting of expert statements in a box, change of font shape and colour. The aim is to make the text more attractive and coherent, e.g. by using standardised markings (shape, colour, bold font) for individual thematic sections.

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

SUMMARY

This article performs a secondary (quantitative and qualitative) content analysis of the available empirical research on perceptions of COVID passports and a discourse analysis of media material from websites to try to determine whether COVID passports were perceived as a symptom of post-pandemic normalisation or rather a planned behavioural intervention.

A main hypothesis was put forward stating that COVID passports were primarily a behavioural intervention instrument to encourage vaccination uptake, leading to far-reaching social change, and three specific hypotheses. All were confirmed by inductive inference based on analysis of empirical studies and discourse study. Hypothesis two (the outcome of the behavioural intervention was the practice of perceiving COVID passports as tools of digital surveillance leading to a loss of personal freedom) was confirmed most strongly, while hypothesis one (the outcome of the behavioural intervention was the practice of perceiving COVID passports as a pass to normality in social life) and hypothesis three (the outcome of the behavioural intervention was the practice of discrimination against the unvaccinated framed as a punishment for avoiding vaccination) were confirmed somewhat less frequently. This distribution indicates not only the perception of COVID passports in the perspective of a government-designed and top-down behavioural intervention, but also citizens' concerns about the monitoring of their social life and fear of losing control of their digital identity and personal freedom.

Public behavioural interventions may be a viable opportunity for authorities to steer social behaviour in a direction that is more conducive to well-being and social order, but they raise a number of important questions about the limits of limiting civil liberties, respect for the dignity of the human person, security, protection and sharing of personal data collected on a large scale, among others. Although education in a behavioural approach is seen as an ineffective tool for behavioural change, it is probably worthwhile to make an effort focused on developing effective information, education and communication strategies to put trust in authorities.

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

SOURCE MATERIAL FOR SOCIOLOGICAL ANALYSIS

European Parliament (2020a). *Public opinion monitoring at a glance in the time of COVID-19: 20 March 2020*. Eurobarometer.

European Parliament (2020b). *Public opinion monitoring at a glance in the time of COVID-19: 27 March 2020*. Eurobarometer.

European Parliament (2020c). *Public opinion monitoring at a glance in the time of COVID-19: 3 April 2020*. Eurobarometer.

European Parliament (2020d). *Public opinion monitoring at a glance in the time of COVID-19: 20 April 2020*. Eurobarometer.

European Parliament (2020e). *Public opinion monitoring at a glance in the time of COVID-19: 27 April 2020*. Eurobarometer.

European Parliament (2020f). *Public opinion monitoring at a glance in the time of COVID-19: 5 May 2020*. Eurobarometer.

European Parliament (2020g). *Public opinion monitoring at a glance in the time of COVID-19: 12 May 2020*. Eurobarometer.

European Parliament (2020h). *Public opinion monitoring at a glance in the time of COVID-19: 19 May 2020*. Eurobarometer.

European Parliament (2020i). *Public opinion monitoring at a glance in the time of COVID-19: 27 May 2020*. Eurobarometer.

European Parliament (2020j). *Public opinion monitoring at a glance in the time of COVID-19: 3 June 2020*. Eurobarometer.

European Parliament (2020k). *Public opinion monitoring at a glance in the time of COVID-19: 9 June 2020*. Eurobarometer.

European Parliament (2020l). *Public opinion monitoring at a glance in the time of COVID-19: 16 June 2020*. Eurobarometer.

European Parliament (2020m). *Public opinion monitoring at a glance in the time of COVID-19: 23 June 2020*. Eurobarometer.

European Parliament (2020n). *Public opinion monitoring at a glance in the time of COVID-19: 1 July 2020*. Eurobarometer.

European Parliament (2020o). *Public opinion monitoring at a glance in the time of COVID-19: 7 July 2020*. Eurobarometer.

European Parliament (2020p). *Public opinion monitoring at a glance in the time of COVID-19: September 2020*. Eurobarometer.

European Parliament (2020r). *Public opinion monitoring at a glance in the time of COVID-19: October 2020*. Eurobarometer.

European Parliament (2020s). *Public opinion monitoring at a glance in the time of COVID-19: December 2020*. Eurobarometer.

European Parliament (2020t). *Public opinion on COVID-19 vaccination. December 2020,* Eurobarometer.

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

European Parliament (2021a). *Public opinion monitoring at a glance in the time of COVID-19: January 2021*. Eurobarometer.

European Parliament (2021b). *Public opinion monitoring at a glance in the time of COVID-19: February 2021*. Eurobarometer.

European Parliament (2021c). *Public opinion monitoring at a glance in the time of COVID-19: March 2021*. Eurobarometer.

European Parliament (2021d). *Public opinion monitoring at a glance in the time of COVID-19: April 2021*. Eurobarometer.

European Parliament (2021e). *Public opinion monitoring at a glance in the time of COVID-19: May 2021*. Eurobarometer.

European Parliament (2021f). *Public opinion monitoring at a glance in the time of COVID-19: June 2021*. Eurobarometer.

European Parliament (2022). *Archive of reports: public opinion monitoring in the time of COVID-19.* Available at: https://www.europarl.europa.eu/at-your-service/pl/be-heard/eurobarometer/public-opinion-in-the-time-of-covid-19 (2020–2024).

Worldometer (2020). *COVID-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/ (01-09-2020).

Worldometer (2021). *COVID-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/ (01-03-2021).

Worldometer (2022). *COVID-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/ (01-03-2022).

SOURCE MATERIAL FOR DISCOURSE ANALYSIS

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8457120,certyfikat-covid-pe-ue.html (PC-1)

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8079775,paszport-covidowy-przywileje-podroze-szczepionka-covid.html (PC-2)

https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8107582,paszporty-szczepien-na-swiecie-dzialaja-w-izraelu-w-ue-sa-w-planach.html (PC-3)

https://www.gazetaprawna.pl/wiadomosci/artykuly/8111869,powrot-do-zycia-tylko-z-zielonym-paszportem.html (PC-4)

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8079775,paszport-covidowy-przywileje-podroze-szczepionka-covid.html (PC-5)

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8148210,stodolak-behawioryzm-medyczny-aparthaid-paszporty-covidowe.html (PC-6)

https://www.rp.pl/zdrowie/art19172241-system-sie-pogubil-przez-do-szczepianie-nie-wszyscy-dostaja-paszport-covidowy (PC-7)

https://www.rp.pl/polityka/art19137551-przepisy-w-unii-europejskiej-certyfikaty-covidowe-pomoga-w-podrozach (PC-8)

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8403358,paszport-covidowy-waznosc-do-kiedy-przedluzenie-bezterminowo.html (PC-9), (PC-10)

https://www.rp.pl/zdrowie/art36104811-polskie-paszporty-covidowe-bez-terminowe-turysci-moga-miec-problemy (PC-11)

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8337398,efekt-paszporty-covidowe-zaszczepienia-zgony-mniejsze-straty-dla-pkb.html (PC-12)

https://www.fakt.pl/polityka/nawet-wsrod-opozycji-nie-ma-porozumienia-co-do-paszportow-covidowych/229bd79?utm_source=www.fakt.pl_viasg_fakt&utm_medium=referal&utm_campaign=leo_automatic&srcc=undefined&utm_v=2 (PC-13)

https://www.fakt.pl/plotki/sebastian-fabijanski-o-paszportach-covid-owych-selekcja-to-jest-zniewolenie/vj8x9wz (PC-14)

https://www.fakt.pl/wydarzenia/paszporty-covidowe-parlament-europejski-podjal-decyzje/zd4ghzr (PC-15)

https://turystyka.rp.pl/popularne-trendy/art36506141-unia-europejska-certyfikaty-covidowe-moga-sie-jeszcze-przydac-przedluzmy-je (PC-16)

https://krytykapolityczna.pl/kraj/milada-jedrysik-michal-sutowski-czwarta-fala-covid-19-polska/ (PC-17)

https://www.fakt.pl/polityka/ekspert-premiera-paszporty-covidowe-przydalby-sie-rowniez-wewnatrz-kraju/hflkjfx (PC-18)

https://www.fakt.pl/pieniadze/certyfikaty-covidowe-na-wakacjach-polski-rzad-przedluza-ich-waznosc/gkzdz98 (PC-19)

BIBLIOGRAPHY

Amadae, S. (2007). Rational Choice Theory. In M. Bevir (ed.), *Encyclopedia of Governance* (pp. 785–791). Sage Publications.

Balfour, R., Bomassi, L., & Martinelli, M. (2022). Coronavirus and the Widening Global North-South Gap. https://carnegieeurope.eu/2022/04/25/coronavirus-and-widening-global-north-south-gap-pub-86891 (25-04-2023).

Bell, G. (2021). #COVIDTIMES: Social experiments, liminality and the COVID-19 pandemic. *Journal & Proceedings of the Royal Society of New South Wales*, *154*(1), 60–68.

Bemelmans-Videc, M.-L. (2007). Introduction. Policy Instruments Choice and Evaluation. In M.-L. Bemelmans-Videc, R. Rist, E. Vedung (Eds), *Carrots, Sticks & Sermons. Policy Instruments and Their Evaluation* (pp. 8–26). Transaction Publishers.

Berelson, B. (1952). *Content Analysis Iin Communication Research*. Free Press.

Bucher, H. J. (2015). Internet discourse as multimedia networked communication. A postulate for paradigm development. In R. Opiłowski, J. Jarosz, & P. Staniewski (Ed.), *Linguistics of the Media. An anthology of translations* (pp. 221–254). ATUT / Neisse Verlag.

Datta, S., & Mullainathan, S. (2012). Behavioural Design. A New Approach to Development Policy. *CGD Policy Paper*, *16*, 1–33.

de Figueiredo, A., Larson, H. J., & Reicher, S. D. (2021). The potential impact of vaccine passports on inclination to accept COVID-19 vaccinations in the United Kingdoms: Evidence from a large cross-sectional survey and modelling study. *EClinicalMedicine*, *40*, 1–10. https://doi.org/10.1016/j.eclinm.2021.101109

Drury, J., Mao, G., John, A., Kamal, A., Rubin, G. J., Stott, C., Vandrevala, T., & Marteau, T. M. (2021). Behavioural responses to Covid-19 health certification: A rapid review. *BMC Public Health*, *21*, 1205. https://doi.org/10.1186/s12889–021–11166–0

European Commission (2022). *EU Digital COVID Certificate*.https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (15-06-2022).

Ferdek, B. (2022) The post-pandemic future of humanity and Christian humanism. *Theology in Poland*, *16*(2), 53–64. https://doi.org/10.31743/twp.2022.16.2.04

Garrett, P., White, J., Dennis, S., Lewandowsky, S., Yang, C-T., Okan, Y., Perfors, A., Little, D., Kozyreva, A., Lorenz-Spreen, P., Kusumi, T., & Kashima, Y. (2021). *Papers Please: Predictive Factors for the Uptake of National and International COVID-19 Immunity and Vaccination Passports*. School of Psychology, The University of Melbourne. https://psyarxiv.com/fxemq/download/?format=pdf (20-02-2024).

GEMIUS (2023, February 8). *Poland Mediapanel survey results for January 2023*. https://www.gemius.pl/wszystkie-artykuly-aktualnosci/wyniki-badania-mediapanel-za-styczen-2023.html (20-04-2023).

Höijer, B. (2011). *Social Representations Theory. A New Theory for Media Research*. *Nordicom Review*, *32*(2), 3–16. https://doi.org/10.1515/nor-2017–0109

Holsti, O. R. (1969). *Content Analysis for Social Science and Humanities*. Addison Wesley.

Itti, L., & Koch, C. (2000). A saliency-based search mechanism for overt and covert shifts of visual attention. *Vision Reserch*, *40*(10–12), 1489–1506. https://doi.org/10.1016/s0042–6989(99)00163–7

Kopytkowska, M., & Kumiega, Ł. (2017). *Critical discourse analysis: contexts, problems, directions of development*. In M. Czyżewski, M. Otrocki, T. Piekot, J. Stachowiak (Eds), *Analyzing public discourse. Review of methods and research perspectives* (pp. 177–207). Academic Publishing House.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology*. Sage Publications.

Krivolap, A. (2022). Glass man identity: From big brother to covid passport. *Studia Humanistyczne AGH*, *21*(2), 31–39. https://doi.org/10.7494/human.2022.21.2.31

Low, D. (2011). Cognition, Choice and Policy Design. In D. Low (Ed.), *Behavioural Economics and Policy Design: Examples from Singapore* (pp. 1–13). World Scientific Publishing Company.

Lunn, P. (2014). *Regulatory Policy and Behavioural Economics*. OECD Publishing.

Momani, B. (2020). *After Covid-19, Will We Live In A Big Brother World*. Centre for International Governance Innovation: University of Waterloo. https://www. cigionline.org/articles/after-covid-19-will-we-live-big-brother-world (26-02-2024).

Moscovici, S. (1984a). The Myth of the Lonely Paradigm: A Rejoinder. *Social Research*, *51*, *939–967*.

Moscovici, S. (1984b). The Phenomenon of Social Representations. In R. M. Farr, & S. Moscovici (Eds), *Social Representations* (pp. 3–69). Cambridge University Press.

Moscovici, S. (1988). Notes Towards a Description of Social Representations. *European Journal of Social Psychology*, *18*, 211–250.

Moscovici, S. (2000). *Social Representations. Explorations in Social Psychology*. Polity Press.

Moscovici, S. (2001). Why a Theory of Social Representations? In K. Deaux & G. Philogéne (Eds), *Representations of the Social: Bridging Theoretical Traditions* (pp 8–35). Blackwell Publishers.

Narożniak, A., & Princ, M. (2022). Vaccine certificate as an instrument of legal regulation of international movement of persons. *Public Law Studies*, *2*(38), 27–59.

Neuendorf, K. A. (2017). *The Content Analysis Guidebook*. Sage Publications.

Olejniczak, K., & Śliwowski, P. (2014). Is a revolution coming? Behavioural analyses in public interventions. In A. Haber, K. Olejniczak (Eds), *(R)evaluation 2. Knowledge in action*. Polish Agency for Enterprise Development.

Omyła-Rudzka, M. (2021). *Poles on vaccination against Covid-19. No. 75.* CEBOS. https://www.cbos.pl/SPISKOM.POL/2021/K_075_21.PDF (20-06-2021).

Shafir, E. (2013). Introduction. In E. Shafir (Ed.), *The Behavioural Foundations of Public Policy* (pp. 1–9). Princeton University Press.

Szulich-Kałuża, J., Sławek-Czochra, M. (2025). Covid passports in Poland and Europe – symptom of post-pandemic normalisation or behavioural intervention? A study based on empirical research and discourse analysis.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 75–100). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Tomasz Bichta

Chair of Political Systems and Human Rights, Institute of Politics and Administration, Faculty of Political Science and Journalism at Maria Curie-Skłodowska University, Lublin
ORCID: 0000-0001-6441-7196

ANGOLA'S HEALTH SECURITY SYSTEM

Abstract: Angola is a model example of an African country which, despite being the focus of interest for China, the USA and other powers, is consumed by all the ills of the continent. In this case, we can also speak of one of the most rapidly developing countries in the world, one of the most expensive, but also one of the most corrupt, where the gap between a handful of the richest and the rest of society is also one of the largest. How does such a situation affect the fulfilment of citizens' crucial need for health care and health security? This article describes the health care system in Angola. Both in legal and institutional terms. The author presents the factual state of affairs in the area of citizens' health security, highlighting the numerous problems, but also attempts to overcome them.

Keywords: Angola, Africa, health care, health security, health system.

In the context of the news that Africa is now one of the most important political and economic centres of the world, Angola is almost a model example to confirm this. On the other hand, it is also a model example of an African state that is consumed by all the ills of the continent. Only that, in this case, we can also speak of one of the world's most rapidly developing countries, one of the most expensive, but also one of the most corrupt.

For a quarter of a century, from independence in 1975 to the beginning of the 21st century, Angola was the scene of one of the bloodiest wars in modern Africa. It is estimated that at least half a million people died in it and the country, a former Portuguese colony, became synonymous with decline. In fact, in

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

the case of Angola, it is difficult to speak of a single war. In fact, three conflicts swept through the territory of the present republic, moving from an anti-colonial phase, through a typically Cold War conflict, to a civil war, whose immediate catalyst was not only ideological differences, but above all the desire for natural resources: diamonds and oil. The conflicts, which lasted a total of 41 years, contributed to the complete breakdown of the political system, the collapse of the social base and economic backwardness.

Angola's recovery from the devastation of the war was helped by oil from the rich deposits of the Angolan shelf. The ruling People's Movement for the Liberation of Angola party, which after the fall of communism transformed itself from a leftist party into a party adhering only to the ideology of staying in power, handed over the oil fields to western companies. Angola soon became the second oil power in Africa after Nigeria and the third richest country on the continent after Nigeria and South Africa – so wealthy that when the economic crisis hit Western Europe, Angola supported the former colonial metropolis, Portugal, with loans.

Angolan wealth, however, has been almost entirely appropriated by the ruling elite, most notably President Jose Eduardo Dos Santos, in power since 1979, and his family and friends. Thanks to petro-profiteers and Western oilmen, Luanda has for years had the reputation of being Africa's most expensive city and Angola one of the most corrupt countries in the world. The World Bank has ranked Angola, with a population of 22 million, among the six countries in the world where the gap between rich and poor is the deepest. To make matters worse, Angola has become hostage to its oil wealth – petrodollars account for more than 90 per cent of its export earnings. It can therefore be said that much depends on oil prices. Its fall on world markets causes a shortage of money in Angola, which in turn affects the citizens. Of course, the poorest suffer the most. The reduction in public spending, for example, is having an impact on the sanitary situation in many poor urban districts of Angola, where there was an outbreak of yellow fever at the end of last year and doctors are reporting increasing numbers of cases of malaria and cholera. The protests of the population are of no avail. Any signs of revolt are severely repressed by the authorities, who seem convinced that it is not support but money that provides real power.

The Constitution adopted in January 2010 defines Angola's political system as a multi-party democracy, based on the coexistence of the executive, legislative and judicial powers. The position of the president is very strong, as he concentrates all executive power in his hands while maintaining de facto independence from the other bodies. The country is divided into 18 provinces, which consists of 157 municipalities. Provincial governors are appointed by the President. Governors of provinces are appointed by the president. Until the early 1990s, Angola had a one-party system in which state structures were subordinate to the ruling MPLA (Movimento Popular para Libertação de Angola – People's Movement for the Liberation of Angola). Power was exercised by the President, the Politburo and the Central Committee. The civil war effectively prevented the construction of a multi-party system, the institutional framework of which was established in the early 1990s. The legacy of the dictatorship and the civil war, which lasted for many years, make the construction of a functioning democratic system one of the greatest challenges facing Angola.

As one can guess, as a result of historical events as well as the current actions (or lack thereof) of the authorities, the health care system in the described country is not at the highest level. In the face of the omnipresent problems in almost all areas of life, health security is also relegated to the background or, at best, is treated by decision-makers on an equal footing with other problems.

Angola's health system consists of a public and private service sector. Under Angolan law, public health services, from primary health care to specialist services, are available free of charge. However, the public system suffers from shortages of doctors, medicines, nurses, care workers, as well as inadequate training and a lack of computerised information to effectively track patients' historical health records. As a result, access to healthcare and pharmaceuticals for the majority of the population is limited. The best quality health services are available in Luanda and other large cities like Benguela, Lobito, Lubango and Huambo. Most of the middle and upper classes use private health services, which usually offer higher quality and fee-for-service care. There are four main private clinics in Luanda: Girassol (linked to state-owned oil company Sonangol), Sagrada

Esperança (linked to state-owned diamond mining company Endiama), Multiperfil (linked to the presidential family) and Luanda Medical Centre. A number of small private clinics are also available. The richest Angolans usually travel to Namibia, South Africa, Cuba, Spain and Portugal for treatment of more complex problems. However, such international health travel is becoming increasingly difficult due to the increased costs associated with the devaluation of the local currency and strict currency exchange restrictions.

The Ministry of Health (MINSA) is the entity responsible for formulating and conducting health security policy. It operates according to the National Health Development Plan (PNDS 2012–2025), which is the main strategic instrument in this matter. However, meeting the need for health security is linked to other social determinants of health, namely nutritional status, conditions of access to drinking water or basic sanitation services. As such, the implementation of health policy requires integration with several areas and levels of government. MINSA works with so-called Health Guardianship Entities, which are autonomous organisations set up directly by the ministry or even more autonomously, registered by the government. These include:

- The National Institute for Health Research (INIS), which is a research institute for technological development and innovation in health care.
- The National Anti-drug Institute (INALUD), which deals with issues relating to the misuse of psychotropic substances, both legally and illegally.
- The National Institute of Opthamology of Angola (IONA), provides healthcare for the prevention, diagnosis and specialised treatment of ocular pathologies.

The National Health System (NHS) comprises the National Health Service, which operates under the supervision and guidance of MINSA and is administered by governors and municipal administrators. The following institutions, which are its sub-systems, are also an important part of the national health system:

- The Health Service of the Angolan Armed Forces (DSS/EMG/FAA), which is the Ministry of Health's largest national partner in community outreach and also provides services to major listed companies (SONANGOL, ENDIAMA and others).

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

- The National Civil Protection Service of the Ministry of the Interior (The National Civil Protection Service – SNPC), which is in charge of coordinating actions in the face of natural disasters and emergencies. It is also responsible for health surveillance interventions organised by the National Police Force in areas related to surveillance, economic activities and border control.
- National Directorate of Public Health (DNSP) – the direct executive service that regulates, directs and coordinates all issues related to disease prevention and control.
- General Health Inspectorate (IGS) – a technical facility and service that monitors, oversees and evaluates the functioning of the National Health System, especially as it relates to the legality of operations, efficiency and service delivery.
- National Directorate of Hospitals – the governing entity that develops policies for public hospitals and coordinates the organisation of health infrastructure.
- Medicines and Health Technologies Regulatory Agency (ARMED) – is a public body with legal personality, endowed with administrative, property and financial autonomy. It is responsible for carrying out regulatory activities, developing guidelines for licensing, inspection and control of activities in the field of medicines and health technologies, in order to guarantee their quality, efficacy and safety.[1]
- Central Medicines Procurement and Supply (CECOMA) – is the public institute responsible for the procurement, distribution and maintenance of medical instruments in coordination with other bodies of the Ministry of Health.
- Other participating entities include hospitals and health care services. These include:
  a) Provincial Health Authorities and the provincial government running the provincial hospitals;
  b) Municipal Health Directorates and Municipal Administrations managing community hospitals, Health Centres and their facilities;

[1] The outpost was established and its terms of reference designated by Angolan Presidential Decree No. 136/21 of 1 June (see Guerra de Almeida, 2021).

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

c) the health education subsystem, which includes a technical and professional group of institutions and public and private medical schools;

d) private and non-profit health services sector (mainly religious institutions and NGOs);

e) Community Development and Health Representatives.

Within the framework of the described system, other government departments also cooperate with the Ministry of Health. In any case, promises of such cooperation can be found in signed agreements and issued legislation. Indeed, in practice, it is not easy to find examples of effective action taken by several ministries.

The right to health care is enshrined in the Angolan Constitution (Biblioteka Sejmowa, 2023). Article 21 provides health care within the framework of the 'Fundamental Tasks of the State,' which include, inter alia, promoting policies to keep primary health care universal and free of charge and making strategic, sustainable investments for the development of human capital, with a particular focus on the full development of children and adolescents, especially in education, health, primary and secondary economy and other sectors. In addition, Article 77(2) of the Constitution guarantees health and social protection.

Angola's National Development Plan 2018–2022[2] (Angola's National Development Plan – PND) and the National Health Development Plan for 2012–2025[3] (National Health Development Plan for 2012–2025 – PNDS) contain the government's priorities for citizens' health security. These include: expanding public health infrastructure and capacity, especially in rural and urban areas with inadequate access to health services; expanding professional training for health professionals; and disease prevention. Angola's health policy development objectives are also included in the government's long-term perspective: Development Strategy 2025, entitled "Angola a Country With A Future Sustainability, Equity and Modernity" (Angola a Country With A Future Sustainability, Equity and Modernity)[4], which aims to "combat poverty and promote the improvement of the health

[2] See further: Cabri, 2023.

[3] See in more detail: República De Angola, 2012.

[4] See República de Angola Ministério do Planeamento, 2007.

status of the Angolan population, providing more direct support to disadvantaged and poor groups, ensuring greater health longevity for the population.[5]"

The aforementioned PNDS 2012–2025 aims to promote respect for the right to health enshrined in the Constitution, universal access to health care, improve the governance and financing mechanisms of the National Health System (NHS), deliver a quality service, combat poverty and improve the well-being of the population. The PNDS has been developed on the basis of priorities for sustainable development. The objectives of this and other government programmes are: to expand and improve access to health care, through the creation, rehabilitation and modernisation of health units and the strengthening of human resources, with a particular focus on Primary Health Care; to promote integrated organisation and cooperation between health units, to ensure the availability of diagnostic resources, the effective management of medicines, vaccines and essential medical devices; to improve and strengthen health care.

Reducing morbidity and mortality from communicable and non-communicable diseases through promotion, prevention, comprehensive treatment and rehabilitation, as well as improving intersectoral interventions on social determinants of health, is also an important objective.

In addition to these strategic guidelines, the Angolan government's understanding of health policy is in line with the objectives of the African Union Agenda 2063,[6] which emphasises, firstly, the need to ensure the health, good nutrition and life expectancy of African citizens. Secondly, it commits to providing citizens with information and quality and affordable health services. The African Union documents identified poverty and hunger and health and nutrition as two key areas of intervention. Not coincidentally, these are among the most important issues facing African countries. Government plans for the development of health security policies place the health of citizens at the top of the needs to be met by those in power. It is recognised as a factor that guarantees state development and social justice. It can therefore be said that, in

[5] *Ibidem*.

[6] See more widely African Union, 2023.

the case of Angola, the first step, i.e. declaring the objectives and acting accordingly, has been taken. The real problem, however, is what comes afterwards, the actual actions. These usually lack the idea, the means and the will. In order to treat the above objectives realistically, attention would have to be paid to a number of elements of health care, which in the case of a well-run state would not be easy, and in a contradiction-torn Angola seems a kind of mission impossible. Such criteria to be considered in health care reform should include:

- Disease control, namely infectious and parasitic diseases and chronic diseases, also with a view to avoiding epidemics.
- Protecting maternal health and supporting birth policies.
- Significant reduction in infant and under-5 mortality.
- Development and organisation of the primary healthcare network taking into account the population and geographical area as well as the specificities of rural and urban areas.
- Expansion of the secondary healthcare network (provincial hospitals) as another priority.
- Creation and consolidation of a tertiary healthcare network (more diversified hospital units) based on both government and private initiative.
- Significant quantitative and qualitative growth in human resources in the health sector.
- Creating an effective health care financing model (public sector).[7]
- Gradual expansion of the organisation and management model of the National Health Fund.

Despite priority declarations, development in the field of health care for Angolan citizens has been very slow. However, it is worth noting the improvement in infant mortality rates (80 per thousand compared to 180 per thousand in 2009) and the decrease in under-five mortality (120 per thousand compared to 300 per thousand at the beginning of the century). There has also been a decrease in the incidence rate of malaria (which fell from 25 per cent to 15 per cent) and leprosy. Polio is a completely eradicated

[7] Public health facilities are mainly funded by the government and to a lesser extent by NGOs. The Angolan government accounts for about 70% of total health expenditure while the rest comes from private sources. See in more detail Health Financing Profile, 2016.

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

disease. The operation to prevent the Ebola virus has been a great success. However, there is still considerable room for progress. There are outbreaks of cholera or yellow fever. Angola still faces malnutrition. Approximately 38% of children show moderate chronic malnutrition and 15% remain with severe malnutrition, which is particularly evident in rural areas. It is noteworthy that, following its experience in combating the Ebola virus, the Angolan government has also taken rapid and fairly effective steps for African countries in combating the COVID epidemic – 19.[8]

Table 1. Selected indicators of the health status of citizens in Angola

1	Life expectancy at birth (years)	63.1
2	Fertility rate	63.6 births per woman
3	Neonatal mortality rate (per 1,000 live births) (2016) 24	24
4	Under-five mortality rate (probability of dying by age 5 per 1,000 live births) (2016)	68
5	Maternal mortality ratio (per 100,000 live births) (2015)	239
6	Diphtheria tetanus toxoid and pertussis (DTP3) immunization coverage among 1-year-olds	31%
7	Infants exclusively breastfed for the first six months of life (%)	38%
8	Child deliveries in health facilities	51%
9	Births attended by skilled health personnel	57%
10	hospital beds per 1,000 people	approximately 0.1

[8] The first case of COVID-19 was reported on 21 March 2020. As of 21 January 2022, the total number of COVID-19 infections was 95,220, 1881 deaths and 86,274 recoveries. The country has 32.11% of the total population vaccinated; 16.80% fully vaccinated and 15.31% partially vaccinated against COVID-19. See *Angola's Health Sector*, 2002, p. 10.

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

11	Doctors per 1,000 inhabitants	about 0.08
12	Nurses per 1,000 inhabitants	0.01
13	Population using improved drinking water sources (%)	13 (Rural) 51.4 (Urban) 36.1 (Total)
14	Population using improved sanitation facilities (%) (2015)	81 (Urban) 60 (Total) 25.9 (Rural)

Source: World Bank Group (2018).

The table above shows the most important health indicators in Angola. Gradually, the quality of health care is improving, but many indicators remain appalling. The government seems to be mindful of the problems, as evidenced by the cooperation that is being established on health care in the broadest sense with Portugal, Brazil or India (*Report on Health Sector…*, 2022, p. 16). It has an increasingly substantive dimension, but is hampered by bureaucratic barriers and perennial internal problems such as corruption. For example, the requirements for international cooperation in the field of health are tightened by many regulations and oblige the parties concerned to obtain many administrative authorisations. Imports of pharmaceutical products are subject to testing during customs clearance as well as post-clearance. Additional supervision is carried out by the Ministry of Trade and Health. In turn, to import medical devices into Angola, a registered importer must submit a Certificate of Origin, a Certificate of Free Sale and a certificate of compliance with the ISO 9001 quality standard to the Ministry of Health, which is responsible for processing the required import licences.

When the Portuguese left Angola in 1975, the African elites were not prepared to take power. Lacking political experience, political vision, but above all the rush for power and to gain control of the wealth, Angola drowned in political chaos. During the period of the People's Republic of Angola, political power was exercised by Presidents Neto and dos Santos and the party nomenklatura, between whom oil revenues were shared. When the 1990s saw a shift away from socialism, the opposition failed to seize power from dos Santos and the political establishment, particularly the provincial governors, who treated the regions as if they were their own farms. On the president's orders, the plundering privatisation of most Angolan state enterprises was also carried out, allowing the ruling class to enrich itself once again. The effects of such policies and rampant corruption can still be seen today.

The biggest losers of 41 years of conflict are above all the Angolans themselves. Society as we understand it today is basically non-existent, mainly due to the fact that in a society dominated by the pursuit of wealth and power, it is these values that matter most. Since 2002, however, there has been a slow rebuilding of social structures and trust in fellow countrymen. Building a new, shared vision of a future Angola therefore becomes quite a challenge in such an antagonised society, which only seven years ago was fighting among itself for money and power. The hope for improving Angola's lot is hailed once again as natural resources, which until recently could only be considered a curse. However, there is a lack of action to diversify the economy, which could result in Angola becoming a so-called 'raw material state' ('petro state'), which functions only on the extraction and export of one or a few natural resources. The neglect of traditional sectors of the economy in pursuit of immediate wealth and satisfaction results in a poor distribution of all the country's natural resources.

Against this background, the poor state of the health service is hardly surprising. Although it is the most important need from the point of view of citizens that they expect the state to meet, in a society divided between the extremely poor and the very rich, those in power push the expectations of the rest into the background. Bureaucracy, corruption, shortages in all sectors certainly do not make the situation any easier. Despite this, Angola's health system seems sufficiently developed to one day, with the right reforms and financial support, be the basis for managing the country's health sector. Change has been very slow for a number of reasons It is telling, however, that in some situations Angola's systemic mechanisms are working very well. This is the case in the fight against the recent pandemic, which has been quite successful because of the experience acquired earlier in the fight against the Ebola virus.[9] It seems that the

[9] See more widely Imf.org, 2020.

key to creating a high level health security system in Angola is to face the remaining problems of the country. However, there are so many of them that, especially in view of the progressive degeneration of the political and social system, this appears to be an impossible task. Perhaps if comprehensive, coordinated and well-considered external assistance were obtained, it would be possible to lift this African country out of its decline. The hope of involving the powers could be the aforementioned raw materials, but the situation we see today shows that neither African decision-makers nor Chinese or American investors care about the right approach. Angola remains a country where the struggle is not for a better tomorrow for its people, but only for wealth and power.

BIBLIOGRAPHY

Angola's Health Sector (2002). AHB Limited.

Bichta, T. (2022). Health safety in Sub-Saharan Africa in the face of the COVID-19 pandemic. In J. Kięczkowska, L. Węgrzyn-Odzioba, A. Wójciszyn-Wasil (eds), *Health Security – Policy – Communication* (pp. 11–33).

Davidson, B. (2011). *Social and political history of Africa in the 20th century.*

Evaluation Report Evaluation of ECHO's Global Plan 2000 – Angola. Sector: Health and Nutrition.

Gulbicka, B. (2013). *Problemy wyżywienia ludności na kontynencie afrykańskim*. Instytut Ekonomiki Rolnictwa i Gospodarki Żywnościowej. Państwowy Instytut Badawczy.

Kłosowicz, R. (2017). *Contexts of dysfunctionality of sub-Saharan African states.*

Leśniewski, M. (2000). Wojna w Angoli (1961–1998). In A. Bartnicki (ed.), *Zarys dziejów Afryki i Azji, Historia konfliktów 1869–2000*. „Książka i Wiedza".

Lizak, W. (2012). *African security institutions.*

Period: January till December (2000). Programme: ECHO/AGO/210/2000/01000, Jarl Chabot, ETC Crystal.

Report on Health Sector in Angola, Embassy of India in Luanda (2022, May). Newsletter, Luanda.

Wilk, W. (2018). *Jobs, population growth, climate change, migration. A proposal for a "Marshall Plan" for Africa*. Polish Centre for International Aid Foundation.

Websites:

African Union (2023). *Agenda 2063: The Africa we want*. https://au.int/en/agenda2063/overview (08–08–2023).

Allianz Care (2023). *Guide to Healthcare in Angola*. https://www.allianz-care.com/en/support/health-and-wellness/national-healthcare-systems/healthcare-in-angola.html (07–23–2023).

Biblioteka Sejmowa (2023). *Constitution of Angola*. https://biblioteka.sejm.gov.pl/konstytucje-swiata-angola/ (08–08–2023).

Cabri (2023). *National Development Plan for Angola (PND 2018–2022)*. https://www.cabri-sbo.org/en/documents/national-development-plan-pnd-2018–2022 (08–08–2023).

Cire.pl (2016, April 2). *Angola. Africa's oil powerhouse breathless*. https://www.cire.pl/artykuly/serwis-informacyjny-cire-24/111213-angola-zadyszka-afrykanskiej-naftowej-potegi (06–08–2023).

Guerra de Almeida, R. (2021, August 25). *Angola, Legal news June and July 2021*. https://www.linkedin.com/pulse/angola-legal-news-june-july-2021-renato-guerra-de-almeida (08–08–2023).

Gutkowska, A. (2007, January 6). *Aleksandra Gutowska: Angola (1992–2002) – Ideology gone, the struggle is for wealth and power*. https://psz.pl//124-polityka/aleksandra-gutowska-angola-1992–2002-ideologia-odeszla-walka-toczy-sie-o-bogactwo-i-wladze (06–08–2023).

Health Financing Profile (2016, May). *Angola*. https://www.healthpolicy-project.com/pubs/7887/Angola_HFP.pdf (08–08–2023).

Imf.org (2020, September 21). *Angola: Confronting the COVID-19 Pandemic and the Oil Price Shock*. https://www.imf.org/en/News/Articles/2020/09/18/na-angola-confronting-the-covid-19-pandemic-and-the-oil-price-shock (10–08–2023).

Investafrica.pl (2023). *Angola on a bumpy development path*. http://www.invest-africa.pl/2012/01/angola-na-wyboistej-sciezce-rozwoju/ (06–08–2023).

Jankowski, D. (2023). *Conflict in Angola*. https://fae.pl/biuletynopinie-konfliktwangolihistoriaterazniejszoscprzyszlosc.pdf (06–08–2023).

Nationsonline.org (2023). *Angola Country Profile – Nations Online Project*. https://www.nationsonline.org/oneworld/angola.html (07–23–2023).

República De Angola (2012). *National Health Development Plan 2012–2025*. https://faolex.fao.org/docs/pdf/ang169620.pdf (08–08–2023).

República de Angola Ministério do Planeamento (2007). *Angola 2025*: *Angola a Country With A Future Sustainability, Equity and Modernity*. https://faolex.fao.org/docs/pdf/ang184675.pdf (08–08–2023).

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Transparency.org (2021). *Corruption Perceptions Index*. https://www.transparency.org/en/cpi/2021/index/ago (08–08–2022).

World Bank Group (2018). *WHO 2018 report and World Bank latest data*. https://databank.worldbank.org/reports.aspx?source=2&country=AGO#advancedDownloadOptions (08–08–2023).

World Bank Group (2023). *Mortality rate, infant (per 1,000 live births) – Angola*. https://data.worldbank.org/indicator/SP.DYN.IMRT.IN?locations=AO (08–08–2023).

Bichta, T. (2025). Angola's health security system.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 101–114). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Justyna Kięczkowska

Institute of International Relations of the Maria Curie-Skłodowska University
E-mail: justyna.kieczkowska@mail.umcs.pl
ORCID: https://orcid.org/0000-0002-9395-2363

Liliana Węgrzyn-Odzioba

Institute of International Relations of the Maria Curie-Skłodowska University
E-mail: liliana.wegrzyn-odzioba@mail.umcs.pl
ORCID: https://orcid.org/0000000238978843

ONLINE CONSULTATION – OPPORTUNITY OR THREAT TO HEALTH SECURITY

Abstract: Online consultation, as a form of remote medical consultation, has gained popularity, especially in the era of the COVID-19 pandemic, offering patients convenient and fast access to healthcare. On the one hand, tele-portfolios allow for the continuation of medical care without the need for the patient to be physically present in the medical facility, which reduces the risk of infection and allows for a faster response to health problems. In addition, they improve the accessibility of specialists, especially in rural areas and for people with limited mobility. On the other hand, online consultation comes with challenges, such as the difficulty of accurate diagnosis without a physical examination, the risk of misjudging health conditions, and issues related to the privacy and security of digitally transmitted medical data. The article analyses these risks and presents best practices and recommendations to minimise the risks, such as the use of advanced security technologies, training for medical staff and appropriate handling procedures. The article concludes that online consultation can represent a significant opportunity for the healthcare system, provided that it is implemented with appropriate security measures and professional ethics to ensure high-quality service delivery and patient protection.

Keywords: online consultation, health security, health system, patient.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

INTRODUCTION

In recent years, telemedicine, and in particular online consultation, has become an integral part of the healthcare system worldwide, including in Poland. Online consultation, defined as a remote medical consultation carried out by means of telecommunication technologies, allows patients to receive medical advice without having to be physically present in the doctor's office. The development of information and communication technologies and the growing demand for efficient and accessible healthcare have contributed to the rapid growth in popularity of online consultation. The COVID-19 pandemic significantly accelerated the adoption of online consultation, especially in Poland. The reduction of face-to-face interpersonal contacts, closing the healthcare system to direct patient contact, encouraged the introduction of alternative forms of healthcare delivery. Online consultation often proved to be the only form of provision in the context of ensuring continuity of healthcare, especially for patients with chronic diseases, the elderly and residents of rural and hard-to-reach areas. Despite the benefits, online consultation also brings with it a number of challenges and potential risks that can affect patient health safety. Lack of face-to-face contact, diagnostic limitations, technical issues and risks related to privacy and data security are just some of the issues that require detailed analysis. The aim of this article is to analyse whether online consultation represents an opportunity or a threat to patient health safety. By reviewing the available data and literature, we will discuss both the benefits and potential risks of online consultation. In particular, the focus is on aspects related to healthcare accessibility, quality of diagnosis, data security and acceptance of this form of consultation by both patients and physicians. The findings presented can help to better understand the role of telereading in the modern healthcare system and identify directions for further development and potential areas that require additional research and regulation.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

ONLINE CONSULTATION – DEFINITIONS

Online consultation is a form of telemedicine that involves the provision of medical advice remotely using telecommunications technology. It is defined as "a remote medical consultation between a patient and a physician or other health professional via electronic communication means such as telephone, video conferencing or online platforms" (Smith, 2020). Online consultation can take different forms, depending on the technology used and the specifics of the consultation. The most common types of telehealth consultations are telephone consultations: this is the simplest form of telehealth, involving a telephone conversation between patient and doctor. This type of consultation is widely available and easy to conduct, but has diagnostic limitations due to the lack of visual assessment of the patient (Brown, 2019). Another type is video consultations. Tele-consultations delivered via videoconferencing, which allow visual assessment of the patient and a more interactive consultation. Through the use of cameras and microphones, doctors can conduct more detailed medical interviews and observe the patient (Jones & Miller, 2019). Asynchronous consultations are also gaining popularity. Online consultations implemented through online platforms where patients can send their symptoms, questions and test results to a doctor who responds at a convenient time. These types of consultations are convenient for patients, but may delay response times to urgent health problems (Lee & Kim, 2019). In the Polish legislation and health care system, online consultation is regulated in several key aspects. The definition of online consultation and the rules for its use are mainly derived from the legislation on telemedicine and health services. In Poland, online consultation is defined and regulated by several legal acts, among others, the Act on Medical Activity of 15 April 2011 (Journal of Laws, 2011, no. 112, item 654), as amended. It introduced the basic regulations on telemedicine, including online consultation. According to this law, health services can be provided by means of electronic communication. In turn, the Regulation of the Minister of Health of 12 August 2020 (Journal of Laws, 2020, item 1395) sets out in detail the rules for the provision of online consultation. This document defines the online consultation as 'a health care service

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

provided with the use of information and communication systems or communication systems that enable communication at a distance between a patient and a doctor or other authorised medical professional'. In Polish law, the key elements of the definition of online consultation should also be set out. Firstly, it is a health service. Online consultation is a form of health benefit, which means that it is a service provided to preserve, save, restore or improve the health of a patient.

The manner in which online consultation is implemented is through ICT systems or communication systems. Online consultation must be implemented through ICT systems (such as the Internet, e-Health platforms) or communication systems (e.g. telephone). It is a form of distance communication, so a key element of tele-treatment is the ability for a patient and a doctor or other authorised health professional to communicate at a distance, without the patient having to be physically present in a medical facility. Medical records regulations are also an important element. Online consultations must be properly documented, just like traditional visits. The medical record should contain information about the course of the tele-treatment, the doctor's recommendations and any prescribed medication.

Polish law also defines the rules for the proper implementation of the online consultation. And in this aspect, it is crucial to specify the practical conditions and requirements. According to Polish regulations, online consultation may be provided by doctors and other authorised medical professionals who are qualified and authorised to practise their profession in Poland. Prior to the provision of an online consultation, the patient must give his or her consent to this form of consultation. The consent may be given orally or in writing, and its form should be properly documented. Online consultation must be carried out in a way that ensures the security and confidentiality of the patient's medical data. The ICT and communications systems used for tele-lectures must meet certain security standards in accordance with data protection legislation (RODO). It is important that the systems used for online consultation ensure that the quality of the connection is adequate so that the consultation can run smoothly. Each online consultation must be properly documented in the patient's medical history. The documentation should include information about the course of the online consultation, the diagnosis made, the medical recommendations and the medication prescribed. The documentation of the online consultation must be kept in accordance with the applicable legislation on the protection of personal data and medical records. Doctors and other medical staff are obliged to maintain the confidentiality of the information obtained during the online consultation, in accordance with the applicable legislation on medical confidentiality. In emergency situations where online consultation is not sufficient to provide adequate medical care, the patient should be advised to contact a medical facility directly or call for medical assistance.

If, for technical or other reasons, online consultation cannot be provided, the patient should be provided with information on alternative forms of obtaining medical assistance (*ibidem*). The definition and principles of providing online consultation in Poland are precisely defined by current legal regulations, which aim to ensure the efficiency and safety of this form of medical service provision. Online consultation, as a remote medical consultation carried out by means of ICT or communication systems, enables patients to obtain medical advice without the need for physical presence in a medical facility.

As of 16 March 2021, restrictions have been placed on the provision of online consultation in primary care in Poland by decree of Minister Adam Niedzielski.[1]

[1] According to the referenced organisational standard for online consultation in primary care, from 16 March 2021, there shall be a restriction of the possibility of performing online consultation : in cases where the patient or his/her legal guardian has not consented to the provision of a service in the form of a online consultation (excluding the issuance of a prescription necessary for the continuation of treatment and an order for the supply of medical devices as a continuation of the supply of medical devices, if this is justified by the patient's state of health reflected in the medical records and excluding the issuance of a certificate); during the first visit carried out by a doctor, nurse or midwife of the Primary Health Care, indicated in the declaration of choice referred to in art. 10 of the Act of 27 October 2017 on Primary Health Care; in connection with a chronic disease in the course of which there has been a worsening or change in symptoms; in connection with a suspected malignant disease; for children under 6 years of age in addition to control advice

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The legal basis for online consultation in Poland sets out in detail the rules for the organisation and implementation of online consultation. These regulations define who is authorised to provide online consultation, how it should be conducted and what technical and organisational requirements must be met. The key elements of the regulations are the qualifications of the medical personnel, the patient's consent, technical preparation, medical documentation and the protection of personal data. Online consultation is used in many areas of medicine, including primary care, chronic disease management, mental health and specialist care. With online consultation, patients in remote locations, those with limited mobility and patients requiring constant monitoring can receive the medical care they need without frequent visits to health facilities (Patel & Jackson, 2022).

Online consultation, of course, offers numerous benefits, including increased accessibility to healthcare, time and cost savings, and increased efficiency when it comes to administrative activities: exemptions, prescriptions, referrals. The data presented in the table illustrate how frequent the use of online consultation is.

Year	Number of online consultations in all types of services	Number of online consultations in POZ
2021	58 662 365	45 585 229
2022	28 513 421	20 961 176
2023	21 220 761	16 358 236
01.–03.2024	5 334 782	4 220 330

Source: Ezdrowie.gov.pl (2024).

during treatment, determined by personal examination of the patient, which can be provided without a physical examination; by a doctor who provides primary health care services, in the context of patient care related to the prevention, prevention and eradication of COVID-19 in relation to children under the age of 2 year of age and in the situation of referral of a patient to undergo home isolation; and when, by a primary care physician, he or she provides the patient, no earlier than on the eighth day of undergoing such isolation, with either an advice or a online consultation during which he or she assesses the patient's state of health, Online consultations from 16 March 2021, https://www.medexpress.pl/blogosfera/teleporady-od-16-marca-2021-r-tylko-poz-z-ograniczeniami-inni-lekarze-bez-ograniczen-80978/ (19–06–2024).

However, the implementation of online consultation also presents some challenges, such as diagnostic limitations, technical issues and the need to ensure a high level of patient data protection. Clearly, this is an important element of a modern healthcare system, the effectiveness of which depends on the proper application of regulations and the adaptation of the technology to the needs of patients and medical staff. As technology develops and regulations continue to improve, online consultation has the potential to become an even more integral and effective form of healthcare delivery in Poland. Online consultation has gained widespread acceptance as a modern and convenient form of medical service delivery, particularly in the context of the COVID-19 pandemic. However, its effective use requires further refinement of the technology, ensuring adequate data security and adapting the healthcare system to new realities. For patients, online consultation is first and foremost a way to access healthcare more easily and quickly, while for healthcare professionals it is a tool for more efficient time management. Key challenges include diagnostic limitations and the need to ensure data privacy and security, which requires constant monitoring and improvement of existing practices and technologies.

The Committee on Medical Ethics of the Supreme Medical Council drafted Article 9 of **the Code of Medical Ethics** in 2023, which was to set out the most important rules regarding online consultation. The Supreme Medical Council proposed the following rules for the provision of online consultation services:

- personal contact between doctor and patient is the most appropriate form of doctor-patient relationship;
- the doctor is required to verify the identity of the patient and to ensure that the conditions of the online consultation are confidential before the provision of the service by online consultation;
- it is the doctor's responsibility to inform the patient of the limitations of online consultation compared to face-to-face contact, and in particular to indicate the symptoms that justify a face-to-face visit or, if necessary, to recommend contact with a medical facility;
- online consultation may be provided, particularly in the treatment of chronic conditions, for consultation in the course of

ongoing treatment or to ensure continuity of treatment until the next possible in-person visit. Online consultation is not recommended for patients who have not yet been treated by a doctor or who present a new health problem;

- it is unacceptable to carry out the patient's diagnosis and treatment only by means of online consultation (*Report. Investigations conducted…*, 2021).

The newly adopted Code of 18.05.2024 did not include such a provision but only stated that it: "The doctor shall choose such a form of consultation (in particular, in-patient visit, online consultation) that ensures the patient the available quality and continuity of medical care" (NIK, 2024).

The legislation on telehealth in Poland is an important step towards modern and socially adapted healthcare. However, it is necessary to continuously monitor and adapt the legislation to changing technological and social conditions in order to ensure the safety, efficiency and high quality of medical services provided.

BENEFITS AND RISKS OF PROVIDING ONLINE CONSULTATION

Powered by rapid technological developments, modern medicine is undergoing a revolution in the way healthcare services are delivered. One of the most innovative solutions that has gained prominence in recent years is online consultation. They are a form of remote medical consultation that allows patients to receive medical advice without the need for physical contact with a doctor. Online consultation not only reflects advances in technology, but also addresses many of the significant challenges of modern healthcare, such as accessibility of services, cost-effectiveness and health and epidemiological safety. By reducing the need to travel to medical facilities and enabling rapid access to medical advice, online consultations address society's growing expectations for easy and rapid access to healthcare.

In this part of the article, I will analyse the main benefits of online consultation as well as the risks. We will focus on aspects such as increased accessibility to specialists, time and cost savings, as well as the impact on health security in the context of the global COVID-19 pandemic, as it seems crucial to present

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

a comprehensive picture of the benefits of online consultation, highlighting its role as part of a modern healthcare system. When analysing the benefits associated with the use of online consultation in the health care system, the first place should be given to the potential of increasing access to medical care, especially for people living in remote regions of the country, characterised by limited mobility. Thus, it should be stated that online consultation eliminates in some way geographical barriers by enabling patients with Internet access to receive medical consultations regardless of their location. People living in smaller towns or villages can obtain medical advice without having to make long journeys to specialists located in large urban centres (Journal of Laws, 2011, No. 112, item 654).

A second important aspect related to improved accessibility is that, thanks to telemedicine, patients can obtain specialist advice more quickly, which is often crucial in cases requiring immediate medical intervention. Waiting times to see a specialist are significantly reduced, which can speed up the diagnostic and therapeutic process (OECD, 2024). Online consultation is also an effective solution for people with limited mobility, who can and most often do find it difficult to access traditional medical facilities on a regular basis. Thanks to telemedicine, older people, people with disabilities or patients after surgery can receive healthcare without having to leave their home (Wright, 2024). Seniors or people with disabilities, in order to stay under medical care, have to go through a series of often strenuous activities beyond their physical capabilities. Many times, in addition to physical dysfunctions dictated by age or illness, there is the inability to obtain support and assistance from other people/family. The specific requirements of this patient group are to be met by online consultation, which offers the possibility of simplifying and speeding up necessary medical procedures. The patient has access to the attending physician as well as to high-level specialists regardless of his or her location. The possibility of direct, quick access to medical services, carrying out urgent consultations with a doctor without the need to leave home and wait in long queues at specialists' offices, make online consultation a very convenient solution for seniors and people with disabilities (Bujanowska-Fedak *et al.*, 2013).

In analysing the benefits of online consultations, it is impossible not to consider their practical application dimension. Online consultation is used in various fields of medicine, including family care, psychiatry, dermatology, paediatrics and many other specialities. Doctors can remotely assess a patient's condition, perform diagnostic consultations, monitor the course of treatment and provide therapeutic advice. For example, in psychiatry, online consultation allows patients to receive regular therapeutic consultations without having to attend the doctor's office in person (Gutiérrez-Rojas *et al.*, 2023). Studies show that patients are satisfied with the ability to receive medical advice quickly without having to wait long for an appointment (Smith & Jones, 2018).

The undoubted benefit, both for doctors and patients when using online consultation, is the time saving. By eliminating the need to travel to a medical facility, it is possible to get help more quickly and reduce the waiting time for a consultation. Online consultation can therefore significantly reduce the time needed to obtain medical advice, which is important especially in emergency cases.

In situations such as an exacerbation of a chronic disease or a sudden injury, a quick remote consultation can be crucial for appropriate clinical case management. Online consultation should enable clinicians to quickly assess the patient's condition and decide on further medical management, which can significantly reduce the time needed to provide assistance. In cases requiring a specialist medical opinion, online consultation allows patients to be referred to the appropriate specialist more quickly. This is particularly important in situations where time is crucial to the effectiveness of treatment, such as in cases of stroke or heart attack (Achenbach, 2024). Cardiac tele-portals allow physicians to monitor patients with heart disease,[2] assess

[2] Electrocardiographic telemonitoring (TM-EKG) using external recorders is a fundamental tool for cardiac telediagnosis and involves the analysis of ECG recordings recorded remotely and transmitted to a surveillance centre. Electrocardiographic telemonitoring makes it possible to detect, document and evaluate abnormal electrical function of the heart during daily activity and increases the chance of an accurate diagnosis. Some TM-EKG devices are also equipped with the ability to monitor, among other things, respiratory function, physical activity, blood pressure (Piotrowicz *et al.*, pp. 698–707).

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

test results and adjust drug therapy in real time. Patients can also receive advice on healthy lifestyles and cardiovascular disease prevention. Debatable yet applicable is the use of tele-portals for oncology patients. Oncologic online consultations enable cancer patients to receive regular oncology consultations, evaluation of laboratory results and monitoring of side effects of cancer therapy. Through telemedicine, patients can receive support and advice on managing their disease symptoms. Online consultations enable doctors to monitor and manage side effects of cancer therapy, such as nausea, pain or fatigue. Through remote consultations, patients can quickly receive advice on symptom relief and treatment changes, significantly improving quality of life. Cancer is often associated with tremendous stress and mental strain for patients. Online consultations can include psychological and psychiatric consultations that support patients to cope with anxiety, depression and other mental health problems associated with the disease (Smith *et al*., 2023).

Online consultation also became an indispensable part of the healthcare system during the Covid-19 pandemic. This time was a period of significant change in the global healthcare system, forcing rapid adaptation and innovation in healthcare delivery. One of the most important tools in the fight against the spread of the virus has just become online consultation, aimed at continuing medical care while minimising the risk of infection. According to health system managers at the state level, online consultation was supposed to eliminate the need for in-person visits to medical facilities, significantly reducing the risk of SARS-CoV-2 virus transmission among both patients and medical staff. Through remote consultations, patients were able to receive the care they needed without having to leave their homes, which was particularly important for those at higher risk (WHO, 2020). Online consultation was also intended to help reduce the number of people physically going to healthcare facilities. Such a solution was expected to reduce the risk of infections within health care facilities and allow health care staff to focus on caring for patients requiring hospitalisation. It is also indicated that online consultation enabled continuity of healthcare even in conditions of lockdown and movement restrictions. Patients were able to continue chronic disease

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

management, specialist consultations and health monitoring without interruption, which was crucial for their health.

Online consultations were expected to make a significant contribution to modern healthcare, particularly in the face of the challenges posed by the COVID-19 pandemic. The stated benefits of online consultations include increased accessibility to healthcare by eliminating geographical barriers and reducing waiting times for consultations. Online consultations provide patients with the opportunity to contact doctors more quickly and easily, virtually 24 hours a day. The effectiveness of tele-portfolios is also reflected in time and cost savings for both patients and medical facilities. Patients can avoid the costs and time associated with travel, and medical facilities can better manage their resources. Indications are that online consultation has the potential to become a sustainable part of healthcare, offering benefits for both patients and the healthcare system. However, despite the numerous benefits, online consultation also carries risks.

Despite its many advantages, online consultation carries significant risks and hazards that require careful analysis and appropriate countermeasures. This section of the article will discuss the main risks associated with the use of online consultation. We will focus on aspects related to healthcare quality, data security, technological barriers and ethical challenges. The analysis of these risks aims to identify areas that need attention and improvement so that online consultation can be used effectively and safely as part of the healthcare system.

In the dimension related to the quality of healthcare, the following risks can be delineated. Firstly, there are limitations in diagnosis. This is one of the main risks associated with online consultation. The limited possibility to perform a full diagnosis, the lack of physical examination of the patient, can lead to diagnostic errors, inappropriate treatment or delayed detection of serious diseases. Research indicates that the lack of face-to-face contact can limit a doctor's ability to fully assess a patient's condition. Diagnostic errors are one of the most common safety issues in ambulatory care, and a virtual visit can increase this risk. During an in-person interaction, the doctor can get a more complete picture of the patient's condition. Furthermore, doctors

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

often rely on other forms of face-to-face interview to fully assess the patient's condition. Observation of body language, personal behaviour and other individual characteristics can provide a more complete picture and reveal opportunities for intervention. In addition, telemedicine visits typically involve interaction between one doctor and the patient, whereas office visits often involve interaction with other healthcare professionals, including nurses, medical assistants and technicians, who can assist in making a definitive diagnosis (Ihi.org, 2022). Another diagnostic risk associated with telemedicine is an over-reliance on technology. Over the past 20 years, healthcare systems have recognised that diagnostic errors often occur when clinicians rely on electronic medical records or other technology during diagnosis. Online consultation can generate the risk of relying on descriptions, charts and patient records for diagnosis. With the relatively limited physical examination possible during a virtual visit, the doctor may be too dependent on the patient's history and laboratory results. Doctors must therefore perform the tele-visit with due diligence, check the information and determine if and when an in-person visit is really necessary. However, it should be emphasised that direct contact with the patient often plays a key role in building the doctor-patient relationship and in understanding subtle health signals. In online consultation it is more difficult to notice some symptoms or they may not be noticed at all. Patients may also feel a lack of trust and security, which can affect the effectiveness of communication and treatment. While telemedicine provides numerous benefits in the delivery of care to patients, it also deprives the interaction of a degree of humanity and depth. Another risk in the area of the quality of telehealth services is therefore the disruption of the doctor-patient relationship. However, bearing in mind that a thorough history and physical examination is not always possible or justifiable for every patient, it is important to remember that the real potential for value lies in the cultivation of the patient-doctor relationship. Both the nature and importance of the physical examination and the full spectrum of the role physicians play in restoring patients to health must not be forgotten (Lapow, 2023). Further evidence of the value of the physical examination is its centrality to preclinical medical

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

education. Learning in the discipline of medical science is not just an academic exercise, but rather a broader education about what it means to be a doctor.

The area of key importance for the proper implementation of online consultation, which at the same time generates the most risks, is that related to data security and privacy. Online consultation involves the transmission and storage of medical data online, which creates the risk of data breaches. Hacking attacks, inadequate system security and human error can lead to the leakage of sensitive patient health information. Ensuring adequate security measures are in place is key to protecting patient privacy. In 2018, cyber-security was identified as one of the biggest industry challenges in the healthcare industry (Healthcare Executive Group, 2018). Since then, the development of the online consultation during the pandemic has highlighted security challenges in healthcare. As of 2020, less than half of providers across the healthcare continuum meet the standards set by the National Institute of Standards and Technology for cybersecurity (Cynergistek, 2020). As virtual care grows in popularity, security measures have not kept pace with the demand for telemedicine services. Cyber-security is not typically a fashionable word in patient safety conversations. However, secure cyber behaviour can protect patient data security (Crystal *et al.*, 2021). Another threat is the diversity of data protection regulations in different countries. It can complicate the international provision of telehealth. Medical facilities need to comply with privacy and data protection regulations, which can be challenging in the context of the globalisation of telemedicine services.

Threats in the area of telehealth use also arise from technological and accessibility barriers. Here, inequalities in access to technology are a serious problem in the first place. When analysing this threat, it is pointed out that there is a group of patients who do not have unequal access to the technology necessary to use online consultation. Older people, those with lower economic status or those living in regions with poor Internet infrastructure are most often excluded from this type of healthcare. This phenomenon, known as 'digital exclusion' (Dijk, 2010), can exacerbate inequalities in access to healthcare.

There are two categories in the catalogue of causes of digital exclusion. The first is infrastructural barriers. These most often relate to restrictions on access to ICT infrastructure, such as apparatus, medical equipment, computer equipment in the broad sense and telephone equipment and networks. This category also includes software, including all kinds of applications, e-services or e-products. Due to the increasing affordability of computer equipment, the growing popularity of mobile devices, the ease of access to the Internet and the dynamic increase in Internet bandwidth (Batorski, 2015), it should be concluded that in the patient group, technological, and therefore financial, limitations will increasingly generate the occurrence of digital exclusion. This problem becomes relevant from the position of healthcare providers. This is because it is they who bear the greatest responsibility related to the implementation, maintenance, development and, consequently, financing of ICT solutions in health care. Financial barriers and difficulties constitute one of the most effective blockades to the implementation of ICT solutions in health care (Korczak, 2014; Korczak, 2016). In the case of the second category, psychological barriers should be pointed out (Stawicka, 2015). These are linked to a lack of digital skills and a lack of motivation (not realising the benefits) to use ICT (Lew-Starowicz & Lorecka, 2013).

There is still a group in society characterised by greater apprehension, lack of motivation, interest, knowledge or skills to use the increasingly available ICT solutions. This situation is created by technological progress, which requires ICT users to constantly update their knowledge and skills. Unfortunately, not everyone, especially not the elderly and senior administrative staff of hospitals, is able to keep up with the dynamic development of ICT. Even the most proficient ICT users sometimes get lost in the flood (noise, overload) of information, unable to find what they were looking for (Fazlagić, 2013). Psychological barriers are much more difficult to overcome than infrastructural barriers and pose serious challenges for decision-makers implementing solutions and technologies in the area of digitisation of the health system.

The risks associated with tele-visits are also the possible medical errors arising during their provision and the determination of

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

liability for them. These are most often more complicated than in traditional visits. Determining who is liable in the event of diagnostic or technical errors is key to protecting both patients and doctors. Some of the most common reasons that can lead to a medical error in the implementation of an online consultation include: lack of prior preparation for the online consultation – providing the service without prior, reminder review of the documentation; failure to take the full necessary medical history – the frequently encountered annotation "not examined"; unreflective continuation of pharmacotherapy under the "prescription ordering" system – the patient asks for a prescription and the doctor, without checking the effects of the previously prescribed medicine, prescribes the medicine again; failure to check the effects of the prescribed therapy – continuation of treatment without check-ups; denying the patient the right to an in-person visit – despite the patient's wish to do so; being relied on by other staff (nurses or registrars) to provide e-prescription codes and recommendations on the use of the prescribed medicines – if the person providing the information makes a mistake, it will be charged to the doctor; an error in the subsequent completion of the documentation – entering data into the electronic system from handwritten notes, after the completion of services, which may result in the data being saved to the wrong patient to whom they belong; this is prevented by the doctor being equipped with devices (headphones, microphone) allowing the conversation to take place and the content to be saved into the computer at the same time. It should be emphasised that the doctor may be liable civilly, before a criminal court or disciplinarily for any adverse consequences for the patient of the inappropriate use or misuse of "remote" or "telephone" treatment (Karkut, 2023).

With regard to risks, it is worth looking at the Ombudsman Report 2019–2021 (*Report. Investigations*..., 2021). In the area of Primary Health Care, in which telehealth is most widely used, 15% of all completed investigations dealt with by the Ombudsman in 2019–2021 were recorded. The most common irregularities cited in the report include lack of access to health services in family medicine and, to a lesser extent, paediatrics. Violations of patient rights were confirmed in 93% of cases. A recurring problem, was primarily:

- not being able to register for an appointment with a primary care doctor, particularly during a pandemic, and being refused in the event of a sudden deterioration in health;
- lack of telephone contact with the facility due to overloading of the telephone line;
- lack of information on the standard of online consultation – patients were not given information on when online consultation could safely replace a face-to-face visit to a doctor and when there were indications for face-to-face contact;
- lack of online consultation, as well as lack of due diligence during online consultation (e.g., despite medical indications, the patient was denied an in-patient visit or information on the condition) (*ibidem*).

At the same time, for the Covid-19 pandemic period, the Ministry of Health and the National Health Fund prepared a report based on a survey of a sample of 13,961 people. This was the largest survey of patient satisfaction with online consultation conducted in Poland. It covered 15,462 patients, of whom as many as 80 percent (14,245 people) had used online consultation in the last four months. 13,961 people agreed to take part in the survey and answer the questions (Koscielniak, 2023). The survey was conducted from 7 July to 1 August 2020. The survey showed that only about 18 percent of patients used an in-person clinic visit during the COVID-19 outbreak. The remainder, nearly 82 percent, were diverted to a remote clinic. The majority of these appointments (81.5 percent) were made in the form of a phone call to a doctor. Only 0.3 percent (45 people taking part in the survey) used a online consultation in the form of a video call. Patients who used online consultation were also asked about the availability of doctors and any problems with the connection. It turned out that 76.4 percent of those surveyed did not have any problems calling the OPD. More than 14 percent needed several attempts, but eventually the online consultation took place. Less successful was e-registration, which was used by 2 percent of respondents. A small group (1.5 percent) of patients said that they did not call in. Almost 6 percent of patients, which shows what absurdities occurred, went to their GP surgery in person to make a tele-registration appointment. 92 percent of those surveyed said that the issue they had called the doctor about was resolved positively. Only 8 percent of patients felt that they needed advice or assistance of another kind (*ibidem*). The majority of respondents found online consultation to be beneficial, substantive and at least as good as in-patient advice. As many as 16 percent of patients felt that online consultation was better than seeing a doctor in person. More than 41 percent of patients said that the quality of e-visits was comparable to an in-person visit; however, as many as one third of those asked believed that a traditional "face-to-face" consultation was better (*ibidem*). A year later, the Polish Society of Family Medicine conducted a similar survey prepared by the same author (Dr Agnieszka Mastalerz-Migas). The survey was aimed at both patients and medical staff; unfortunately, the results of this survey are not available.

SUMMARY

Online consultation, despite its many advantages, brings with it a number of risks that need to be properly managed. Diagnostic limitations, risk of data breaches, technological barriers and ethical challenges are just some of the issues that need attention. It is most important to ensure adequate security measures, patient and physician education and the creation of inclusive telemedicine systems.

In the future, further developments in technology and the adaptation of regulations can help minimise these risks, making online consultation a safer and more effective tool in healthcare. For several years, the Ministry of Health has been organising Telemedicine Round Table meetings to develop and elaborate high standards for telemedicine services. Currently, the Home Medical Care project is being implemented and developed, which makes it possible to carry out a number of examinations at home to correctly diagnose the patient's state of health. Currently, it is possible to auscultate the heart and lungs and perform spirometry; soon it will be possible to perform imaging examinations of the ear, throat, skin and whole body. In combination with online consultation, it can provide an alternative and complement to the traditional patient-doctor interaction. However, for online consultation to realise its full potential, it is necessary

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

to address and minimise the associated risks. Challenges such as difficulties in accurate diagnosis, the risk of misdiagnosis, and risks related to the privacy and security of medical data require special attention. It is therefore important to implement advanced security technologies, training for medical staff and appropriate operating procedures to ensure the protection of patient data and the high quality of services provided.

BIBLIOGRAPHY

Achenbach, S. J. (2020). Telemedicine: Benefits, Challenges, and its Great Potential. *Health Law and Policy Brief*, *14*(1), Article 2. https://core.ac.uk/download/pdf/288206664.pdf (23–06–2024).

Act on therapeutic activity of 15 April 2011 (2011). *Journal of Laws*, *112*, item 654.

Act on therapeutic activity of 15 April 2011, Dz. U. 2011, no 112 item 654.

Batorski, D. (2015). Technologies and media in the homes and lives of Poles. In J. Czapiński, T. Panek (eds), *Diagnoza społeczna 2015. Warunki i jakość życia Polaków*. Rada Monitoringu Społecznego.

Brown, L. (2019). Telephone Consultations in Modern Healthcare. *Health Communication*, *33*(2), 145–158.

Bujnowska-Fedak, M. M., Kumięga, P., & Sapilak, B. J. (2013). Application of modern telemedicine systems in the care of elderly people. *Family Medicine & Primary Care Review*, *15*(3), 441–446. https://bibliotekanauki.pl/articles/552297.pdf (23–06–2024).

Crystal, T., Fausett, M., Christovich, M. P., Parker, J. M., Baker, J. M., & Keebler, J. R. (2021). Telemedicine Security: Challenges and Solutions. *Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care*, *10*(1), 340–344. https://doi.org/10.1177/2327857921101241 (Original work published 2021).

Cynergistek (2020, September 17). *The direction. Annual Report, 2020.* https://www.facebook.com/cynergistek/ (25–06–2024).

Dijk, J. (2010). *Społeczne aspekty nowych mediów*. PWN.

Ezdrowie.gov.pl (2024, June 10). *Telporada in POZ*. https://ezdrowie.gov.pl/19836 (02–06–2024).

Fazlagić, J. (2014). *Innovative knowledge management*. Difin Publishing House.

Gov.pl (2021). *Report. Investigations by the Patient Ombudsman into individual cases in 2019–2021.* https://www.gov.pl/web/rpp/raport-postepowania-wyjasniajace-prowadzone-przez-rzecznikapraw-pacjenta-w-sprawach-indywidualnych-w-latach-2019–2021 (24–06–2024).

Gutiérrez-Rojas, L., Alvarez-Mon, M. A., Bernabeu, Á. A., Capitán, L., De las Cuevas, C., Carlos Gómez, J., Grande, I., Hidalgo-Mazzei, D., Mateos, R., Moreno-Gea, P., De Vicente-Muñoz, T., & Ferre, F. (2023). Telepsychiatry: the future is already present. *Spanish Journal of Psychiatry and Mental Health*, *16*(1), 51–57.

Healthcare Executive Group (2018). *HCEG top 10*. https://hceg.org/hceg-top-ten/ (25–06–2024).

Ihi.org (2022, June 23). *Telemedicine and the Challenge of Diagnostic Accuracy*. https://www.ihi.org/insights/telemedicine-and-challenge-diagnostic-accuracy (25–06–2024).

Jones, B., & Miller, C. (2021). Telemedicine: Past, Present, and Future. *Health Technology*, *33*(4), 567–579.

Karkut, A. (2023). *Online consultation – mistakes most commonly made by doctors*. https://pulsmedycyny.pl/teleporady-bledy-najczesciej-popelniane-przez-lekarzy-1109170 (26–06–2024).

Korczak, K. (2014). *Internet-based tools to support health care*. Wolters Kluwer SA.

Korczak, K. (2016). Games for health – concept, examples of application and socio-economic potential. *Rocznik Kolegium Analiz Ekonomicznych*, *42*.

Kościelniak, P. (2023). *Poles are satisfied with online consultation – MZ and NFZ survey*. http://forumezdrowia.pl/info/opinie/polacy-sa-zadowoleni-z-teleporad-badanie-mz-i-nfz/ (23–06–2024).

Lapow, J. (2023). *Telemedicine, PPE, and COVID-19: A New Paradigm for the Patient-Physician Relationship*. https://roundtablejournal.org/2020/11/28/telemedicine-ppe-and-covid-19-a-new-paradigm-for-the-patient-physician-relationship/ (25–06–2024).

Lee, J., & Kim, S. (2019). Advantages of Telehealth in Modern Medicine. *Medical Innovations*, *29*(2), 89–97.

Lew-Starowicz, R., & Lorecka, K. (2013). *Włączenie cyfrowe – droga do reintegracji społecznej*. Wydawnictwa Uniwersytetu Warszawskiego.

Modoro, M. (2021, March 15). *Online consultation from 16 March 2021 only POZ with restrictions, other doctors without restrictions*. https://www.medexpress.pl/blogosfera/teleporady-od-16-marca-2021-r-tylko-poz-z-ograniczeniami-inni-lekarze-bez-ograniczen-80978/ (19–06–2024).

NIK. (2024, May 24). *Code of Medical Ethics*. https://nil.org.pl/izba/krajowy-zjazd-lekarzy/nadzwyczajny-xvi-krajowy-zjazd-lekarzy/8487-nowelizacja-kodeksu-etyki-lekarskiej-kamien-milowy-dla-srodowiska-lekarskiego (23–06–2024).

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

OECD (2024). *The impact of telemedicine on health care system performance*. https://www.oecd-ilibrary.org/sites/d158593d-en/index.html?itemId=/content/component/d158593d-en (20–06–2024).

Ordinance of the Minister of Health of 12 August 2020 on the organisation and delivery of health services using information and communication systems or systems (2020). *Journal of Laws*, item 1395.

Patel, R., & Jackson, L. (2022). Telehealth During COVID-19: A Review of Benefits and Barriers. *Global Health Review*, *56*(1), 45–58.

Piotrowicz, R., Krzesiński, P., Balsam, P., Kempa, M., Główczyński, R., Grabowski, M., Kołtowski, Ł., Lewicka, E., Pelle, M., Piotrowicz, E., Podolec, J., Stańczyk, A., Zajde, J., & Opolski, G. (2018). Telemedicine solutions in cardiology – expert opinion of the Informatics and Telemedicine Committee of the Polish Society of Cardiology, Section of Noninvasive Electrocardiology and Telemedicine of the Polish Society of Cardiology and the Committee of Clinical Sciences of the Polish Academy of Sciences. *Kardiologia Polska*, *76*(3), 698–707. https://doi.org/10.5603/KP.a2018.0058

Report – Investigations conducted by the Patient Ombudsman in individual cases in 2019–2021 (2021). file:///C:/Users/zsm/Downloads/Postepowania_wyjasniajace_2019–2021_e.pdf (24–06–2024).

Smith, A. (2020). The Impact of Telehealth on Patient Care. *Journal of Telemedicine*, *45*(3), 123–134.

Smith, A. & Jones, B. (2018). Patient Satisfaction with Telemedicine Services. *Journal of Health Communication*, *25*(1).

Smith, S. J., Smith, A. B., Kennett, W., & Vinod, S. K. (2024). *Exploring cancer patients', caregivers', and clinicians' utilisation and experiences of telehealth services during COVID-19: A qualitative study*. https://www.sciencedirect.com/science/article/pii/S0738399122002634 (23–06–2024).

Stawicka, A. (2015). *Digital exclusion in Poland, Thematic studies OT-637*. Biuro Analiz i Dokumentacji, Chancellery of the Senate.

WHO (2020, November 13). *Implementing telemedicine services during COVID-19: Guiding principles and considerations for a stepwise approach*. https://www.who.int/publications/i/item/WPR-DSE-2020–032 (26–06–2024).

Wright, E. *Telemedicine and Accessibility for Patients with Disabilities*. https://www.rcmd.com/blog/telemedicine-and-accessibility-for-patients-with-disabilities (20–06–2024).

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Online consultation – opportunity or threat to health security.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 115–135). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Justyna Kięczkowska

Institute for International Relations of the Maria Curie-Skłodowska University,
E-mail: justyna.kieczkowska@mail.umcs.pl
ORCID: https://orcid.org/0000-0002-9395-2363

Liliana Węgrzyn-Odzioba

Institute for International Relations of the Maria Curie-Skłodowska University,
E-mail: liliana.wegrzyn-odzioba@mail.umcs.pl
ORCID: https://orcid.org/0000000238978843

SECURITY OF MEDICAL DATA IN POLAND AFTER THE COVID-19 PANDEMIC

Abstract: The COVID-19 pandemic has profoundly transformed the healthcare landscape in Poland, exposing systemic weaknesses while accelerating the digitalisation of medical services. This article examines the evolving strategy for securing medical data in the post-pandemic era, focusing on both legal and technological dimensions. It highlights the growing threats to patient data, such as ransomware, phishing, insider breaches, and DDoS attacks, which have become increasingly prevalent in Polish medical institutions. The authors analyse key innovations introduced to strengthen data protection, including cloud computing, advanced encryption systems, multi-factor authentication, artificial intelligence, and blockchain. The study also reviews Polish and EU legal frameworks, such as the GDPR and national regulations concerning electronic medical records. Special attention is given to the importance of staff training, patient awareness, and organisational resilience. The article concludes that a comprehensive, technologically advanced, and legally compliant approach is essential for ensuring the long-term security of medical data in Poland.

Keywords: medical data security, COVID-19 pandemic, cyber threats, healthcare digitalisation, cloud computing.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

INTRODUCTION

Hailed as a global event, the COVID-19 pandemic has had a profound impact on all aspects of social and economic life. In the health sector, it has not only caused a huge burden on health systems. In the case of Poland, it has exposed its dysfunctions and shortcomings but also forced an accelerated digitalisation of medical services. In Poland, as in many other countries, medical facilities had to adapt quickly to the new realities, introducing remote consultations, telemedicine and other innovative technological solutions. These changes, while bringing many benefits, at the same time posed new challenges, especially in the area of the security of medical data understood as both 'health data' and 'personal data' of patients. Thus, the security of medical data has become an important issue. Healthcare systems have started to store and process increasing amounts of patients' personal and health data in electronic form. The processing of this data in the cloud, the use of mobile applications for health monitoring and remote medical consultations have increased the risk of data security breaches. Furthermore, the evidently increased number of cyberattacks targeting the health sector during the pandemic demonstrated the importance of implementing effective data protection mechanisms. The COVID-19 pandemic highlighted a number of weaknesses in existing security systems, which forced medical facilities and regulators to take strong steps to strengthen data protection. In Poland, it was necessary to adapt to new legal requirements, such as RODO (Regulation on the Protection of Personal Data) or other solutions currently being introduced by the European Union, and to implement modern technologies to secure medical data. The development of telemedicine, which has since become an integral part of modern healthcare, has been associated with the need to ensure secure data transfer between patients and medical facilities. Remote medical consultations, while extremely convenient and efficient, have created new challenges in ensuring the confidentiality and integrity of health data. The introduction of advanced technologies such as end-to-end encryption, multi-level authentication systems and artificial intelligence for threat detection have become essential to meet the growing security demands.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The aim of this article is to present the evolution of the medical data security strategy in Poland after the COVID-19 pandemic, to identify the main challenges and to discuss innovative approaches and technologies for the protection of patient data. The analysis will cover both changes in legal regulations and practical solutions used by medical facilities to ensure data security. In addition, the article will focus on the long-term consequences of the pandemic on medical data protection and future developments in this area. Medical data security in the post-pandemic era is an extremely important topic, requiring constant attention and adaptation to changing conditions. In the face of increasing cyber threats and the growing volume of data being processed, it is crucial for medical facilities and regulators to be proactive with innovative technological solutions and to raise user awareness of data protection best practices. This article aims to initiate a discussion on current challenges and future trends in medical data security in Poland after the COVID-19 pandemic.

THREATS TO THE SECURITY OF MEDICAL DATA

The healthcare system and the elements that function within it have now become a major target for cybercriminals, both in Poland and globally. In Poland, 43 hacking attacks on medical facilities were reported in 2023, while in 2021 there were only 13 (an increase of more than 300%). Globally, on the other hand, hacking attacks in healthcare are estimated to reach a figure of 1,800 per week (a 74% increase on 2022) (poradyodo.pl, 2023). The low number of reports should not be an indication of a low level of threat; it is instead an indication of low detection of attacks. Attacks on medical data are the type of threat that has not previously been a priority for extensive protection; hence, attacks on this sector have been very effective and have had long-term negative consequences. Hospitals and other healthcare providers process patients' personal data, such as name, PESEL or home address, including sensitive data on patients' health status. Cybercriminals encounter no resistance and have little difficulty in breaching security measures which are still not at an adequate level (or which are often lacking) regarding personal

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

data. Even more frequently, it turns out that it is the human being and his or her mistakes that prove to be the weakest link in the system, as it has repeatedly turned out that, in spite of the conducted training, employees have carelessly handled the entrusted equipment and data, e.g. by providing remote access to computers to unauthorised persons or by activating suspicious links from e-mails that landed in the institutions' mailboxes. Based on the 2018–2022 reports of the President of the Office for the Protection of Personal Data (UODO) and her own experience, Bożena Chmielewska has compiled a catalogue of the most common personal data protection violations in the medical sector:

- sending correspondence containing personal data both in traditional form and to an electronic mailbox to the wrong recipient,
- sending electronic correspondence with unencrypted attachments containing patient test results or copies of medical records,
- disclosure to the wrong person – sharing patient data (or releasing medical records) without checking that the person receiving the records is authorised to receive them,
- issuing and dispensing a prescription to another patient – no patient verification,
- conversion of documentation by patients in physiotherapy practices,
- hooking up individual results to another patient's record and issuing them to the wrong patient,
- mistakes/errors in the patient's chart – e.g. entries in the chart relating to a different patient, entry by a doctor of the wrong PESEL number on a referral for examination,
- failure to verify the identity of the patient – giving the wrong person the service,
- providing patient information by telephone without verifying the identity of the callers and without checking that they are entitled to obtain patient information,
- paper records lost or stolen – carrying records to home visits and leaving them in a shop, office 'on the way',
- paper or electronic records on media – left in an unsecured location – cabinets left open, keys left in cabinet doors, paper records inserted in doors and left unattended, medical records stored in open cabinets or on shelves without the ability to be locked,

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

- loss or theft of a data carrier/access device (laptop) – unencrypted equipment left unattended in a car,
- destruction of medical records by pouring coffee,
- processing of patients' personal data by unauthorised personnel of the treatment facility – lack of authorisations granted by the controller,
- sharing of staff's logins and passwords to IT systems with colleagues,
- operating IT systems on someone else's login – unauthorised access to patient data and unauthorised entry in medical records,
- unauthorised acquisition of image data – recording on a surveillance video the course of dental treatment without prior notification to the patient and without the patient's consent,
- lack of information clauses regarding the use of video surveillance in the establishment,
- hacking attacks – malware that interferes with the confidentiality, integrity or availability of data and unauthorised access to information by breaching security, extorting *ransomware* (*ransomware*),
- leaving access rights to IT systems to employees who have left the medical facility,
- loud conversations and remarks by staff about patients, gossiping about patients and colleagues outside the workplace, making it possible to identify the people being discussed,
- the provision of patient information by unauthorised persons – e.g. cleaning staff,
- retention of medical records for a period of time not in compliance with the Act on Patients' Rights and Patients' Ombudsman (Data Protection Violations in Medical Facilities) (oil.lodz.pl., 2023).

The growing scale of the threat of hacking attacks in hospitals and medical facilities has prompted a response from the EU institution ENISA, the European Network and Information Security Agency. After analysing hacking attacks in EU countries from January 2021 to March 2023, it prepared a report entitled 'Health Threat Landscape' (ENISA, 2024). The report clearly states that one of the main cyber threats in healthcare is ransomware, which accounts for 54% of all security incidents. As many as 43% of incidents among ransomware attacks resulted

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

in a data breach (Poradyodo.pl, 2023). Ransomware is a type of malware that encrypts a victim's data and then demands a ransom to unlock it. The medical sector is particularly vulnerable to this type of attack due to the need for uninterrupted access to patient data. An example is the ransomware attack on the UK's NHS system in 2017, which caused disruption to many medical facilities, negatively impacting patient care. The NHS was hit hard by the WannaCry ransomware attack, which disrupted around 81 NHS branches and 600 primary care organisations. The cost of this cyberattack was estimated at $115m (£86m) and resulted in the cancellation of more than 19,000 appointments (UK equivalent of NHS, 2024).

Another threat to the healthcare system and medical data is phishing attacks. Phishing is a fraudulent method of sending fraudulent emails to phish for sensitive information such as passwords or credit card details. In a medical context, phishing can lead to unauthorised access to information systems, which can result in the theft of medical data. Among facilities attacked by hackers, more than half (54 percent) have just fallen victim to phishing, according to Fortinet's 'IT security in the healthcare sector' study (Marszycki, 2024). In the case of phishing messages, facility employees who unknowingly allow access to systems or databases are identified as the weakest link.

At the level of Polish hospitals, software vulnerabilities that can be exploited, for example with code to launch an attack or gain unauthorised access, are also a serious threat. As long as the flaw is not remedied, a hacker can affect the programme, database, computer or network. Unauthorised access can also be an insider threat, originating directly from the healthcare facility. Insider threats involve healthcare facility employees who may gain unauthorised access to medical data. This can be the result of both deliberate action and unconscious error. An example is the situation of an employee who accidentally shared confidential information on a public network drive (Łokaj, 2016). Another form of threat related to accessing data can also be simply the theft of mobile devices, such as laptops, tablets or smartphones, with medical data. The theft of such devices can lead to data loss if they are not adequately secured, for example through encryption.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

DDOs attacks on hospitals increased in 2023. The pro-Russian group Killnet, is increasingly attacking hospitals, cyber security experts warn. Their speciality is DDoS (a type of attack, e.g. on a server or website, which generates artificial traffic so as to use up all the victim's free resources and make services unavailable. As a result, users are unable to access, for example, a particular website or platform), resulting in the inability to access a system with, for example, patient data. Killnet attacked healthcare organisation websites, starting its campaign in February 2023 and targeting hospitals in more than 25 states in the US. According to Microsoft analysts, as recently as November 2022, 10–20 attacks per day could be seen, while February already saw 40–60 per day. Nearly one-third of these affected pharmacies, hospitals (26 percent), health insurance (16 percent) and healthcare services and care (16 percent) (Cyber 360, 2023). Poland also has a problem of DDOs cyberattacks on hospitals. On Monday 6 February 2023 there were problems with the internal systems of the Central Clinical Hospital in Łódź. The facility's website and email inbox stopped working. An official letter confirmed that an attack had taken place. In November 2022, the Polish Mother's Memorial Health Institute fell victim to a cyberattack. The facility was forced to switch to a traditional paper-based mode of operation. The incident caused difficulties in the operation of the hospital, which of course was most acute for patients (Cyberdefence24.pl, 2023). Microsoft experts point out that this type of activity is increasingly being used as a distraction to hide more sophisticated operations (e.g. data theft) being conducted at the same time (Palczewski, 2024). On 19 March 2024, patient data of the DCG Medical Centre in Wrocław was leaked. The security measures used by the software provider Medily were breached. DCG patients received SMS messages informing them of unauthorised access to a range of data. Amongst other things, names, PESEL numbers, contact details and information about appointments and health status fell into the wrong hands. The case was reported to law enforcement (Testarmy.com, 2024).

Data security may also be lost or compromised as a result of misconduct by staff in a hospital or other health care facility. Incorrect approaches to data protection by staff can also lead to data breaches, resulting primarily in the disclosure of data to unauthorised persons. According to the 2019 NIK report, there are situations where a patient accidentally received the medical records of another outpatient clinic patient, and a man with a mental disorder stole three patient files from the registration room, two of which were not recovered. Cases are also mentioned where copies of medical records were made available to unauthorised persons by the persons to whom the records pertained; in other cases, records were issued without first verifying that the person receiving them was indeed authorised to do so. In data protection, the organisation of a proper process of granting authorisations to process personal data is also an important issue (Topyla, 2024). The NIK report indicated that there were situations in which authorisations were granted to too broad a group of people, i.e. service employees such as a nurse or a room attendant. On the other hand, one could notice the practice of not giving authorisations to people who should have such authorisations – e.g. doctors or nurses. Mistakes also consisted in giving access authorisations to IT systems processing personal data by IT without the prior consent of the hospital director or not removing IT system authorisations from people leaving the hospital. The report showed that some employees had administrator privileges for IT systems processing personal data, even though no such duties were implied in their terms of reference. Such arrangements increased the risk of malicious software being installed on the computers they used. It also identified situations where the antivirus system was not used at all in hospitals or had an outdated virus database (nik.gov.pl, 2019).

A significant problem is the non-use of any authorisation data for access in computer operating systems or the use of the same data – NIK showed that often employees used the same logins and passwords. Such behaviour results in the impossibility to determine which employee performed certain operations in the system (including, e.g. a breach of personal data protection), as well as the impossibility, for example, to revoke access rights of former employees. The Supreme Audit Office also pointed out irregularities in the safeguards applied or problems in the application of safeguards specified in internal regulations: inadequate strength of passwords (e.g. too few characters or passwords of the

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Alice123 type), failure to change the password after 30 days in accordance with internally adopted requirements and failure to block the system in the event of entering an incorrect password several times, inadequate security of the server room, storage of security copies in the same place as the source data (*ibidem*).

Medical data, due to its sensitivity and value, is particularly vulnerable to various types of attacks, such as ransomware, phishing, and unauthorised access.

These threats can lead to serious consequences for patients, such as loss of privacy and health risks, as well as for medical institutions, which may incur costs related to data breaches, loss of public trust and criminal prosecution. In the face of increasing threats, medical institutions must constantly adapt their protection strategies. Data encryption, security policies, staff training and regular audits and updates are just some of the many tools that can contribute to the security of medical data. In the digital age, a dynamic and tailored approach to data protection is essential to ensure patient privacy and the integrity and availability of critical medical information.

CHANGES IN HEALTH DATA SECURITY STRATEGIES

In this age of rapid digitisation, the protection of medical data is becoming an increasingly complex issue. Medical data, containing personal information and patient health details, is some of the most sensitive and valuable data that must be carefully protected from a variety of threats. The COVID-19 pandemic has significantly accelerated the digital transformation in the health sector, forcing medical facilities around the world, including Poland, to rapidly implement modern technologies and adapt to new data security challenges. It has also created specific conditions in which medical facilities have had to quickly adapt to remote working and telemedicine. Solutions that had previously been implemented gradually now had to be implemented on an accelerated basis. The need to ensure secure data transmission, secure ICT systems and protect against cyberattacks became a priority for medical facilities. In Poland, the pandemic highlighted the weaknesses of existing data protection systems and

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

initiated the need to revise and strengthen security strategies. The ground breaking changes included not only technical aspects of security, but also legal regulations and operational procedures. The introduction of advanced encryption systems, migration to the cloud, the use of multi-level authentication and the integration of artificial intelligence in threat monitoring have become essential elements of modern medical data protection strategies.

One of the most important aspects of these changes has been the need to comply with stringent legal requirements such as RODO (the Data Protection Regulation), which impose strict obligations regarding the processing, storage and protection of personal data. The pandemic has also accelerated the need to educate and raise awareness among medical staff and patients on data security best practices.

An important trend in medical data security strategies has been the increased use of cloud technology. Moving medical data to the cloud has enabled medical facilities to manage data more efficiently and provide better protection against data loss. Cloud computing offers scalability, flexibility and advanced security tools such as data encryption and access control, which are key to protecting medical data.

Scaling resources, is particularly important in the health sector, where the volume of medical data can grow rapidly. With the cloud, medical facilities can easily adapt their resources to their current needs without having to invest in costly on-premises infrastructure. One of the main advantages of cloud solutions is, above all, data security. Transferring personal and medical data to cloud computing (a professional, properly secured server room and under the care of full-time administrators), results in a level of security that is unattainable for small and medium-sized entities, and difficult to achieve and requires huge investments in the case of institutions with an extensive organisational structure. Another important advantage of cloud computing is data availability. Cloud solutions allow users to securely access data on any computer and anywhere in the world, which translates into flexibility for the institution's operations. The use of cloud computing also reduces the cost and time of software implementation in the organisation. A healthcare organisation is not forced to expand its IT and network structure, which saves both time and

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

money on IT support. The staff is thus able to fully focus on their activities related to patient care and the quality of services provided, and outsources IT infrastructure security issues to an external company (Dziembek & Bajdor, 2018)

The practical transfer of data to the cloud meant that establishments could avoid unauthorised access and loss of data in the event of failure or theft, for example. It should be emphasised that the computers in the organisation are merely terminal devices with which users log on to individual system accounts and, using a web interface, can read and write data stored on external servers. (Kasza *et al*., 2018). This situation eliminates the risks associated with the fact that in the event of a computer or hard drive failure in the organisation, the data stored on it will be irretrievably lost. The process of accessing the data took place and is still taking place via the Internet, using an encrypted communication channel that provides security at an analogous level to, for example, online banking access. It should also be emphasised that the data stored in the cloud are of a distributed nature, which means that even in the event of a physical loss of data (e.g. theft of hard disks from the server room – data centre), the recovery of such data by unauthorised persons will not be possible. All data stored on cloud servers is also encrypted (mediporta.pl, 2018).

An example of medical cloud success is the case of Spoedtestcorona (e-health ecosystem, now easly.nl). The company was working on a secure solution to allow people in the Netherlands and Belgium to distribute medical tests quickly and without contact, and in 2020, due to the outbreak of the Covid-19 pandemic, they had to churn out an application – an e-health ecosystem – in a very short time and on different platforms. Thanks to Amazon Web Services' cloud computing, they managed to release the application within the agreed deadline of two weeks while maintaining the highest security standards and recorded great success (more than 2 million Covid-19 tests, less than 2,000 other tests conducted quickly and under the right conditions) (mindboxgroup.com, 2023).

Despite resistance from more conservative-minded hospitals, the road to digitalisation and migration to the cloud is only a matter of time. Everything was accelerated, of course, by the

Covid-19 pandemic, and although the mobilisation associated with this event has subsided, there is clearly a growth in technology, remote solutions and cloud computing providing opportunities for AI or IoT (*ibidem*). In the case of Poland, the government website reads that, "Currently, government cloud services are not provided to any healthcare entity, and although the resolution allows for this possibility, other government systems are the priority." According to the Prime Minister's Office, "a government cloud is a type of cloud computing that is used by governments or government agencies to store, manage and share data and applications". It is an easy, fast and user-friendly solution. However, for hospitals in Poland, they will have to meet certain conditions to qualify for the government cloud. However, the Chancellery of the Prime Minister states that "the catalogue of entities eligible to use the RChO in accordance with the resolution includes, among others, independent public healthcare institutions".

The most important principles for qualification include:

- confirming the need for government cloud security level safeguards i.e. in line with the National Cyber Security Standards;
- the possibility of applying a cost-sharing model for the use of services, i.e. the release of the limit of the budgetary part by the relevant authorising officer on a multiannual basis;
- the criticality of the recipient system in terms of the public tasks supported;
- availability of technical resources.

However, if a healthcare facility qualifies for RChO, it will be eligible for a range of solutions (Mieczkowska, 2023). The future of cloud computing in medicine is promising, especially in terms of integration with new technologies such as artificial intelligence (AI), the Internet of things (IoT) and blockchain. AI and IoT can greatly enhance data analytics and patient health monitoring, while blockchain offers an additional level of security and data integrity.

In order to realise the full potential of cloud computing, medical facilities need to continue to invest in staff education and awareness and work with trusted cloud providers. This will ensure the highest level of protection for patient data and further improve healthcare services. The introduction of advanced

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

cloud technologies not only improves data security, but also contributes to innovation and progress in the healthcare sector.

The protection of medical data is a fundamental part of modern information management in the health sector. Medical data is used by a wide range of stakeholders, from hospitals and clinics to individual doctors and patients. Due to their sensitive nature, ensuring their security against unauthorised access and cyberattacks is a priority. In recent years, with the increasing importance of digitisation and remote medical services, the introduction of advanced encryption systems has become an essential step in protecting medical data.

With encryption, medical information stored in information systems is transformed into a form that is unreadable by unauthorised persons. Only those with the correct decryption key can recover the original content of the data. In the context of regulations such as RODO, which impose stringent requirements on the protection of personal data, encryption is a fundamental part of ensuring compliance. The increase in the number of cyberattacks especially during and immediately after pandemic periods on healthcare sectors, highlights the need for advanced security mechanisms. Encryption of medical data protects it from unauthorised access in the event of a security breach of IT systems. Encryption techniques such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) provide a high level of protection and are widely used in securing sensitive information. Even in the event of physical theft of storage media, such as laptops or hard drives, the encrypted information remains protected (Schneier, 2015).

End-to-end encryption (E2E), is the most effective way to protect medical data. In this model, data is encrypted on the source device and remains encrypted until it reaches the destination device, where it is decrypted. This ensures that, even if the data is intercepted during transmission, it remains unreadable by third parties. E2E is particularly important in the context of telemedicine and data exchange between different systems. In contrast, encryption of data at rest (i.e. during storage) and in motion (i.e. during transmission) is essential for comprehensive medical data protection. Encryption at rest ensures that data stored on server disks or terminal devices is secure, while encryption in

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

motion protects data transmitted over communication networks. In practice, the use of both methods provides more complete security (Azaria *et al*, 2016). Secure management of encryption keys is an essential element of an encryption strategy. Encryption keys must be adequately protected to prevent unauthorised use. Today's solutions use hardware security modules (HSMs) and cloud-based solutions to manage keys, providing an additional level of protection (ssl.com, 2024).

Medical data security strategies consistently require change and adaptation to new conditions, one of which was the implementation of multi-level authentication systems. In traditional password-based authentication methods, in the face of the growth and advanced methods of cybercriminals, threats began to be recognised. Commonly used passwords are additionally vulnerable to brute force and phishing attacks, and this requires additional protection measures such as password complexity policies and regular password changes. As a result, healthcare facilities have started to introduce two-factor authentication (2FA) and biometric authentication methods, such as fingerprints or facial recognition, for example. These methods are proving effective in blocking access to sensitive medical data for those not authorised to read and process it. In the process of protecting medical data, authorisation and authentication play a fundamental role. This is the process of verifying the identity of a user or system in relation to granting access to resources. Two-factor authentication (2FA) requires the user to confirm their identity using two independent methods, for example a password and a code sent to a mobile phone. This method significantly increases the level of security, minimising the risk of access by unauthorised persons even if the password is lost or stolen. Authorisation, on the other hand, is the process of granting or denying access to resources based on the identity of the authenticated user. Thus, authentication is related to ensuring that users only have access to data that is necessary to perform their professional duties. Of course, in medical institutions, managing authentication and authorisation especially in large facilities with hundreds of users can be complicated. Therefore, so-called scalable solutions are being introduced where automated identity management (IAM) systems can help manage access and enhance operational efficiency (Suleski *et al.*, 2021).

Existing mechanisms at the same time need to be flexible and technologically advanced enough to keep up with dynamically changing needs and regulations (Stallings & Brown, 2017).

The implementation of multi-level authentication (MFA) systems involves certain costs, both direct (purchase of hardware, software licences) and indirect (staff training, integration with existing systems). Medical facilities need to carefully evaluate the costs of implementing and maintaining this solution to minimise the budgetary impact. Another challenge is to ensure that the usability of IT systems and the user experience are not negatively affected by the introduction of MFA. A successful MFA implementation should be balanced so that the additional layers of security do not impede the day-to-day work of medical staff. Ease of use and quick access to systems is key. Integrating MFA with existing IT systems in medical facilities can be complex and time-consuming. It requires careful planning to ensure compatibility and minimal disruption to systems. Working with experienced MFA solution providers can help ensure smooth integration and avoid technical issues. As cyber threats continue to escalate, MFA can be expected to become the standard in healthcare. More and more regulations and industry standards will require the implementation of multi-level authentication systems to ensure the highest level of protection for patient data (Familoni & Babatunde, 2024).

The use of automation and artificial intelligence (AI) in healthcare data protection has become the next step in security strategies. AI-based systems can analyse vast amounts of data and identify potential threats in real time. Machine learning algorithms are able to detect unauthorised activities and anomalies that may indicate attempts to breach security. Automating security processes allows for faster incident response and reduces the risk of human error. AI can take over many routine tasks that would be time-consuming and error-prone if performed manually. For example, AI-based systems can automatically classify and analyse data, identifying potential threats and minimising the risk of human error. Techniques such as machine learning allow systems to learn and adapt to new threats, making detection and response to security incidents more effective. Machine learning algorithms used by AI can analyse huge sets of medical data to look for hidden

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

relationships and trends – it would take a human being much longer to perform the same action on such a large volume of data. The analysis performed by AI is also expected to enable a better understanding of patients' health status and reduce possible health risks. Artificial intelligence can assist medical staff in making interpretations of the collected medical data through clinical decision support systems (White Paper, 2023). Through the analysis of historical data and the latest scientific research, the results of which are available to AI-enabled systems, when used appropriately, AI is expected to provide physicians with recommendations for diagnosis, treatment and the delivery of patient care, ultimately contributing to the quality of healthcare in a healthcare provider (medidesk.pl, 2023a). AI can be used for predictive analytics to identify potential risks before they occur when it comes to data security. Predictive systems use historical security incident data to create models that predict future attacks. This allows preventative measures to be implemented proactively, significantly reducing the risk of data breaches.

AI and its use is seen as having the potential to dramatically change the landscape of medicine, benefiting both patients and healthcare providers. However, the key to success will be the responsible and thoughtful implementation of these technologies, taking into account all the challenges and potential risks that may arise along the way, which, with the current state of many healthcare systems, seems like a breakneck task.

Another solution used to protect data is blockchain technology, initially known for cryptocurrencies such as Bitcoin. It has found its way into many other fields, including medical data protection. It is characterised by decentralisation, transparency and a high level of security, making it an ideal tool for managing sensitive medical information. Blockchain is nothing more than a distributed database that stores information in cryptographically linked blocks. Each block contains a set of data and new blocks are added to the chain in a linear and chronological manner. A distinctive feature of blockchain is that once stored, data is virtually impossible to change without modifying all subsequent blocks, ensuring high integrity and security of the information. One of the biggest challenges in protecting medical data is ensuring its security and integrity (Zyskind *et al.*, 2025). Blockchain offers a solution through its built-in cryptographic mechanisms that protect data from unauthorised access and manipulation. Due to its decentralised structure, there is no single point of failure, which further enhances resilience against cyberattacks. It also provides full transparency of records, which is crucial in medicine, where accuracy and traceability of data changes are extremely important. Every operation is recorded and can be verified at any time, which facilitates auditing and ensures compliance with regulations such as RODO or HIPAA (Azaria *et al.*, 2016). Blockchain can be used to securely store and share patient data between different medical facilities. An example is the MedRec project (MedRec, 2023), which uses blockchain to manage medical records, providing patients with control over their data and allowing doctors to access a patient's full medical history. In the context of healthcare, blockchain can also be used to track the supply chain of medicines, which is crucial in the fight against counterfeit medicines. The technology enables full transparency and tracking of every stage of production and distribution, which increases security and confidence in the authenticity of pharmaceutical products (Krasowski, 2024). In the context of the application of blockchain in the pharmaceutical industry, Amgen, Sanofi and Pfizer have been the most talked about companies for several years now. These companies have joined forces to work on using blockchain to build a transparent control system for clinical trials of new drugs. Blockchain is expected to help both track and tag trial data records, secure patient information and ultimately speed up the entire process and reduce drug development costs. Pfizer is also implementing another blockchain project – joining forces with AbbVie, McKesson and Roche in working on a tool to align compliance and regulatory requirements and prevent counterfeit drugs from entering the supply chain (*ibidem*).

Blockchain technology has the potential to significantly improve the security and management of medical data. With its unique features such as decentralisation, transparency and cryptographic security, blockchain offers new opportunities in protecting medical information from breaches and unauthorised access. Despite some implementation challenges, the benefits of blockchain in healthcare are invaluable. The future of this technology in medicine looks promising, especially in the context of integration with other modern technologies and the development of appropriate regulatory standards.

LEGAL SOLUTIONS

The COVID-19 pandemic has also influenced the acceleration of the introduction and strengthening of regulations related to the protection of medical data. The computerisation of healthcare and the introduction of Electronic Medical Records (EDM) from 1 July 2021 was intended to facilitate access to records for those authorised to access them. In Poland, the obligation to store medical records in electronic form had already been introduced earlier under the provisions of the Healthcare Information System Act in 2011, while full implementation had just started on 1 July 2021. In turn, the Regulation of the Ministry of Health of 6 April 2020 on types, scope and specimens of medical records and the manner of their processing in paragraph 4. indicated two conditions that must be met in order to consider the records as secured. These are:

- ensuring accessibility for authorised persons only,
- the use of methods and measures for the protection of records whose effectiveness over time is widely recognised (medidesk.pl, 2023b).

Under paragraph 5. medical entities were required to:

- ongoing analysis of current risks and taking action to minimise them,
- the development and application of procedures for safeguarding records and the systems used to process them,
- providing contemporary security measures that are appropriate to current threats,
- ensuring that the software used in the organisation is kept up to date,
- to control the functioning and assess the effectiveness of both organisational and technical/IT security measures,
- planning and implementing long-term records retention plans (*ibidem*).

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

The legislation also regulates who can access, make and amend the records. First and foremost, it is the patient to whom these records relate and the person authorised by the patient who can view the records via an online Patient Account. In April 2023, there were 17 million active accounts. Secondly, the people who produce the medical records have access to them. This is therefore the medical staff with whom the person to whom the documentation relates has contact. The nurse, midwife or doctor providing primary care and medical staff in the context of continuing treatment, or in a life-threatening situation, are also authorised to see them. The patient can also consent to access his or her records for the doctor and the medical facility that did not produce the records – through his or her IKP account. Unfortunately, the EDM project is still not fully implemented mainly due to concerns about the security of data processing and circulation, but also the lack of sanctions from the Ministry for non-compliance by medical facilities. There have been calls for the establishment of professional regional repositories to ensure security and appropriate technical conditions. On this occasion, there was also an offer from the Polish National Cloud, which valued the monthly cost of data storage for medical entities at PLN 500.

Another solution is the introduction of the provisions of RODO (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). Article 4 para. 15, the RODO defines health data as "personal data about the physical or mental health of an individual – including the use of healthcare services – revealing information about health status". Within the framework of the RODO, the EU legislator noted that personal health data should include all data about the health of the data subject, revealing information about the past, present or future physical or mental health of the data subject. This information also includes information collected during registration for and the provision of healthcare services, information derived from laboratory or medical examinations of body parts or bodily fluids, including genetic data and biological samples, and any information about a disease, disability, disease

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

risk, medical history, clinical treatment, physiological or biomedical condition of a person, as well as a number, symbol or other indication assigned to a specific person to uniquely identify that person for health purposes, e.g. the DILO card number. At the same time, the source of the data is irrelevant, i.e., irrespective of who obtained the data and with what device: it may be a doctor or other health professional, a medical device, a diagnostic test, a medical procedure e.g. in vitro.

The new legislation has placed the onus on medical facilities to conduct detailed risk analyses, implement appropriate security measures and regularly monitor and report on data security incidents. With regard to medical data, the DPA establishes specific provisions for sensitive data, which includes health data. The RODO places a very strong emphasis on data privacy and anonymity and provides for high financial penalties for breaches. The RODO introduced the Register of Processing Activities (RCP) which is a key tool to support personal data controllers in organising and monitoring their processing, enabling them to confirm compliance with the principle of accountability. It is another tool to support the security of data storage and processing. The register of processing activities is a document in which information is updated on, among other things, for what purposes personal data are processed, who the data concerns, what is the scope of the data, to whom it is disclosed, until when it will be stored (Articles 32 and 49 RODO). Another element related to RODO is the 'Code of Conduct for the Healthcare Sector' prepared by the Polish Federation of Hospitals and approved in December 2023 by the President of the Office for Personal Data Protection (UODO). The document contains rules for the processing of personal data in medical facilities, indicating minimum requirements and promoting a risk-based approach, with the possibility of monitoring compliance with the code and sanctions for violations, with the aim of increasing the level of protection of personal data in accordance with RODO (udo.gov.pl, 2021).

With regard to the use of artificial intelligence, the Artificial Intelligence Act 2023 was passed which is part of a broader package of policy measures to support the development of trustworthy artificial intelligence, which also includes the Artificial Intelligence Innovation Package and the Coordinated Plan on Artificial

Intelligence. The regulatory framework identifies four levels of risk for artificial intelligence systems: unacceptable risk, high risk, limited risk and minimal risk (digital-strategy.ec.europa.eu, 2024). In February 2024, the European Artificial Intelligence Authority was established within the European Commission. Its purpose is to oversee, together with the Member States, the enforcement and implementation of the Artificial Intelligence Act. Its aim is to create an environment where AI technologies respect human dignity, rights and trust. The introduction of such solutions strengthens all the more the possibility and potential use of AI in health and medical data protection systems. The proposed mechanisms define potential problems and, interestingly enough, the act itself has been formulated, as it were, for the future with enough flexibility to take into account the dynamics of change regarding the development of artificial intelligence. Another forward-looking initiative is the Spring 2024 agreement, in which the European Parliament and the Council approved the Commission's proposal for a European Health Data Space. This will enable individuals to control their health data and facilitate the exchange of data for the provision of healthcare services across the EU, help create a true single market for electronic health record systems, provide a consistent, reliable and efficient system for the use of health data for research, innovation, policy-making and regulatory action. It will be built on: General Data Protection Regulation (RODO), Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, Data Act [Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828], the NIS Directive [Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security within the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS Directive 2)]. These acts provide a horizontal framework of rules applicable to the health sector. The European Health Data Space, on the other hand, will allow the creation of specific sectoral legislation, taking into account the sensitivity of health data.

The construction of the European Health Data Space will require significant development work. To support this, the Commission will co-finance, among others:

- HealthData@EU pilot project,
- Xt-EHR Joint Action (through direct grants to Member States),
- infrastructure development (health.ec.europa.eu, 2024).

Legal solutions at the European Union level, as well as correlated Polish regulations, are clearly aimed at securing the entire area of medical data, while being aware of the development and dynamics of change, and at the same time meeting modern technologies.

A significant aspect of the changes in medical data security strategies has been increased user awareness and education. Medical facilities have invested in training programmes for medical staff and patient awareness campaigns to raise awareness of cyber security risks and data protection best practices. Regular training and security testing has become standard, helping to reduce the risk of human error and unauthorised activities. Education and awareness of medical data security is essential to effectively protect sensitive information from threats such as cyberattacks, unauthorised access and human error.

Human error is one of the main causes of healthcare data security breaches. Healthcare professionals who are not adequately trained in information security principles may unknowingly make mistakes such as inappropriately sharing information, using weak passwords or opening malicious email attachments. Healthcare data security education aims to minimise such risks by raising user awareness of best practice and potential risks. Employees who are aware of the risks and know how to defend against them are more likely to follow safe practices and report security incidents.

One of the main challenges in employee education is resistance to change. Employees can and often are reluctant to adopt new procedures and technologies, especially if they perceive them to be complicated or time-consuming. To overcome resistance, it is important and appropriate to engage management and run awareness campaigns that expose the benefits of data security compliance. The cyber threat landscape is dynamic and constantly evolving, which means that education programmes need to be regularly updated to keep up with new forms of attacks and methods of protection. This means that threats need to

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic. In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

be constantly monitored and training programmes need to be adapted to the current situation (cez.gov.pl, 2023).

The future of healthcare data security education lies in personalised training programmes that are tailored to the individual needs and proficiency level of employees. Personalised training can increase learning and participant engagement, resulting in better security compliance. Globalisation and international cooperation in data security can lead to the sharing of best practices and educational standards. Healthcare organisations can benefit from the experiences of other countries to help develop more effective educational programmes.

Implemented changes in healthcare data security strategies, ranging from advanced technology, decentralisation of systems, user education and regulatory compliance, are delivering tangible benefits in the form of increased protection of patient data. While the challenges of protecting medical data are significant and constantly evolving, the right strategies and measures can significantly reduce the risk of security breaches. The key to success is a holistic approach that combines technology, processes and people into one cohesive healthcare data protection system.

BIBLIOGRAPHY

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). *MedRec: Using Blockchain for Medical Data Access and Permission Management*. 2016 2nd International Conference on Open and Big Data (OBD). https://doi.org/10.1109/OBD.2016.11

Cez.gov.pl (2023). *Centre for e-Health*. https://cez.gov.pl/pl/page/o-akademii/szkolenia-z-edm (2024–07–07).

Cyber 360 (2023). *Report, Cyber threats to healthcare*. https://ossp.pl/wp-content/uploads/2023/06/Raport-cyberbezpieczenstwo-sluzba-zdrowia-Q12023.pdf (26–06–2024).

Cyberdefence24.pl (2023, March 20). *Pro-Russian hackers increasingly attacking hospitals. The scale of DDoS is growing*. https://cyberdefence24.pl/cyberbezpieczenstwo/prorosyjscy-hakerzy-coraz-czesciej-atakuja-szpitale-rosnie-skala-ddos (25–06–2024).

Digital-strategy.ec.europa.eu (2024). *Shaping Europe's Digital Future, State of the Digital Decade*. https://digital-strategy.ec.europa.eu/pl/policies/regulatory-framework-ai (04–07–2024).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber-security within the Union.

Dziembek, D., & Bajdor, P. (2018). Use of cloud computing in enterprises – preliminary research results. *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, *368*, 27–53.

ENISA (2024). *Health Threat Landscape Report*. https://www.enisa.europa.eu/publications/health-threat-landscape (23–06–2024).

Familoni, B. T., & Babatunde, S. O. (2024). User experience (UX) design in medical products: theoretical foundations and development best practices. *Engineering Science & Technology Journal*, *5*(3), 1125–1148.

Health.ec.europa.eu (2024). *European Health Data Space*. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_pl (05–07–2024).

Icm.edu.pl (2023). *White Paper. AI in health, applying artificial intelligence to the delivery of health services*. https://icm.edu.pl/wp-content/AI%20i%20zarz%C4%85dzanie%20danymi%20w%20plac%C3%B3wkach%20medycznychuploads/2021/06/BIA_A-KSIE_GA_AI-W-ZDROWIU_2022.pdf (30–06–2024).

Kasza, S., Romaszewski, A., Kopanski, Z., Uracz, W., Furmanik, F., Dyl, S., & Tabak, J. (2018). Problems in the dissemination of large cluster analysis in health care. *Journal of Clinical Healthcare*, *3*, 6–33.

Krasowski, M. (2024). *Tech pharma, how blockchain technology affects the pharmaceutical market*. https://przemyslfarmaceutyczny.pl/artykul/tech-pharma-jak-technologia-blockchain-wplywa-na-rynek-farmaceutyczny/ (02–07–2024).

Łokaj, M. (2016). *Access to medical data by non-medical staff – terms of reference and limitations*. https://www.prawo.pl/zdrowie/dostep-do-danych-medycznych-przez-personel-niemedyczny-zakres-uprawnien-i-ograniczenia,262125.html (24–06–2024).

Marszycki, M. (2022, October 11). *What is the state of IT security in Polish hospitals?* https://itwiz.pl/jak-wyglada-stan-bezpieczenstwa-it-w-polskich-szpitalach/ (25–06–2024).

Medidesk.pl (2023a). *AI and data management in medical facilities*. https://medidesk.pl/ai-i-zarzadzanie-danymi-w-placowkach-medycznych/ (01–07–2024).

Medidesk.pl (2023b). *Electronic health data security*. https://medidesk.pl/elektroniczna-dokumentacja-medyczna-a-bezpieczenstwo-danych/ (03–06–2024).

Mediporta.pl (2018, June 14). *Data security in the cloud*. https://www.mediporta.pl/blog/bezpieczenstwo-danych-w-chmurze/ (27–06–2024).

MedRec (2023). *Projects*. https://www.medrec.org/projects (01–07–2024).

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Mieczkowska, K. (2023, August 27). *Government Cloud Computing*. https://www.rynekzdrowia.pl/E-zdrowie/Rzadowa-chmura-obliczeniowa-nie-dla-szpitali-Priorytetem-sa-inne-systemy-administracji,248857,7.html (28–05–2024).

Mindboxgroup.com (2023, August 18). *Cloud computing in the medical sector: innovations and challenges*. https://mindboxgroup.com/pl/chmura-obliczeniowa-w-sektorze-medycznym-innowacje-i-wyzwania/ (28–06–2024).

Nik.gov.pl (2019, November 14). *RODO in Hospital*. https://www.nik.gov.pl/aktualnosci/rodo-w-szpitalu.html (27–06–2024).

Obslugaprzychodni.pl (2022). *Encryption of medical data*. https://obslugaprzychodni.pl/2024/07/21/szyfrowanie-danych-medycznych/ (29–06–2024).

Oil.lodz.pl (2023, March, 22). *Personal data protection violations in medical facilities*. https://oil.lodz.pl/aktualnosci/wszystkie-informacje/najnowsze/naruszenia-ochrony-danych-osobowych-w-placowkach-medycznych.html (20–06–2024).

Palczewski, S. (2023, March 4). *#CyberMagazine: What is DDoS? These attacks are plaguing Poland*. https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-co-to-jest-ddos-te-ataki-nekaja-polske (26–06–2024).

Poradyodo.pl (2023, November 21). *Cyber security in hospitals and other medical facilities – more and more hacking attacks*. https://www.poradyodo.pl/ado/cyberbezpieczenstwo-w-szpitalach-i-innych-placowkach-medycznych-coraz-wiecej-atakow-hakerskich-12463.html accessed 20.06.2024.

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.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data.

Regulation of the Ministry of Health of 6 April 2020 on the types, scope and models of medical records and the manner of their processing.

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.20*.

Ssl.com (2024, May 3). *Best practices in key management*. https://www.ssl.com/pl/artyku%C5%82/najlepsze-praktyki-w-zakresie-kluczowego-zarz%C4%85dzania%2C-praktyczny-przewodnik/ (29–06–2024).

Stallings, W., & Brown, L. (2017). *Computer Security: Principles and Practice*.

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Suleski, T., Mohiuddin, A., Wencheng, Y., & Wang, E. (2021). *A review of multi-factor authentication in the Internet of Healthcare Things*. https://doi.org/10.1177/20552076231177144

Testarmy.com (2024, March 27). *Cyber security in the health sector. Examples and implications*. https://testarmy.com/pl/blog/cyberbezpieczenstwo-w-sektorze-ochrony-zdrowia-przyklady-i-skutki (24–06–2024).

Topyła, M. (2019, November 14). *Personal data protection in hospitals, typical mistakes*. https://kancelariatopyla.pl/ochrona-danych-osobowych-w-szpitalach-typowe-bledy/ (26–06–2024).

Udo.gov.pl (2021). *Protection Code for the Health Sector*. www.udo.gov.pl (04–06–2024).

UK equivalent of the National Health Service (2024).

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralising Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27

Kięczkowska, J., Węgrzyn-Odzioba, L. (2025). Security of medical data in Poland after the Covid-19 pandemic.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 137–162). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Stanisław Bichta

Faculty of Political Science and Journalism, Maria Curie-Skłodowska University
E-mail: Stas.bi@o2.pl
ORCID: http://orcid.org/0009-0008-0414-2387

E-PUBLIC RELATIONS IN HEALTHCARE AND ASSOCIATED RISKS

Abstract: The health service is an area that does not appear to the average citizen as a place that is particularly linked to the Internet and therefore susceptible to various threats. However, the dynamics of the modern world also make it almost necessary for healthcare institutions to conduct public relations activities on the Internet. Of course, as with ordinary web use, there are many risks involved. This article describes the above-mentioned phenomena and attempts to answer the question: do such activities, which are threatened by many dangers, both for patients and for the health service, make sense and should they be carried out?

Keywords: public relations, Internet PR, healthcare, public relations in healthcare facilities, risks in e-PR activities.

INTRODUCTION

In our everyday life we are exposed to many attractive offers coming from various sources. We usually reject such calls or delete e-mails in the knowledge that the content is simply spam and an attempt to trick us into spending money. There are also much more dangerous attempts to extort money or steal our secret data in order to commit crimes. These types of activities are linked to the fact that our lives are wrapped up in various technologies, networks and systems that require us to leave data there. But when we manage to fend off such a hacking attack on our bank

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

account or toss another email into the spam folder, it probably rarely occurs to us to think that our data might have been stolen from healthcare facilities. We tend to suspect telephone networks or banks of this, but the vision of a GP trading in patient data does not cross our minds. And probably rightly so. It is hard to imagine. But it is much easier to accept the fact that a surgery, clinic or hospital has fallen victim to hackers who have stolen patient data from it. Information is the most valuable asset today. These practices are occurring with increasing frequency around the world. This is due to the fact that healthcare is one of the most recent areas to exist on the Internet in various ways, which makes it easier to access the data held by the various facilities. Additionally, this area of our lives, by its very nature, seemed to be free from any kind of cybercrime, and systems to secure it are only just emerging.

It therefore appears that we are dealing in this area with activities that are potentially mutually exclusive. On the one hand, healthcare facilities want to keep up with patients' expectations and be able to 'effectively' advertise and market their services through an online presence. On the other hand, the fact that they are using online activities immediately exposes them to various risks and even attacks. Such dissonance is not unusual, however, as it affects virtually every area of life in the modern world. Only a few questions remain: Is it worth "pushing" the Internet by force within such a sensitive sphere of services as health care? What measures should be taken to establish an effective presence there? What can be done to avoid the countless risks? Is the use of e-PR worth the risks involved?

PUBLIC RELATIONS, E-PR AND HEALTH CARE – DEFINITIONAL ISSUES

The concept of public relations is defined in many ways (Lazorko & Syrkiewicz-Świtała, 2011; Tworzydło, 2003; Przybylski, 2006). This is due to the fact that this type of activity is undergoing a process of significant transformation all over the world. There is a constant search for areas in which it can be applied and, in turn, the characteristics of the increasingly different markets in

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

which public relations activities are implemented are also forcing changes in this field of knowledge. Each definition, however, recognises that it is a specific activity aimed at creating a positive image and building links with the environment. The purpose of public relations is to gain acceptance and goodwill for the actions of an organisation (e.g. a doctor's surgery) and to create and then maintain favourable conditions for its operation. Krystyna Wójcik put the issue in an interesting way, stating that it is a "conscious, purposeful, planned, systematic and long-term impact of organisations, authorities and associations on the public, i.e. the environment. This impact is directed at shaping a specific quality of relations and arrangements by means of communicating and nurturing contacts and subordinating these influences to ethical principles" (Wójcik, 2015). Patients today expect marketing-oriented actions from doctors, healthcare institutions and other institutions related to the market of medical services, because they are used to such practices when using commercial products. Of course, the specifics of the health care sphere do not allow such a literal treatment of medical services, but many tools are allowed. Besides, in health care, public relations can be defined not only as the activities of individual institutions or doctors, but also organisations promoting health or prevention programmes (Łazorko & Syrkiewicz-Świtała, 2011).

Many of these tools are applied through the prism of the Internet. We are then dealing with e-PR or Internet public relations. It is a way of creating the image of a given entity on the Internet using tools available on the web. The main objective of e-PR is broadly understood communication with recipients, building a positive image of the company or product and brand recognition among Internet users, which at the same time is also associated with further development of e.g. the company. The increasing use of the Internet in promotional activities is a consequence of several factors. On the one hand, it is about the expectations and increasing awareness of consumers, their education and access to the web. On the other hand, it is about the activities of, in our case, healthcare institutions, which face the challenge of dynamic technological development and, in order to keep up with changes and expectations, must adapt their activities to the requirements of the market.

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Health care is a well-known term. Sometimes the term "health service" is used interchangeably for this term, but as linguists and specialists point out, it is slowly becoming obsolete and the correct term is health care (Szarkowska, 2022). "Health care" defines the function of the objective and indicates the subjectivity of all stakeholders in the health care process, i.e. the patient himself, medical personnel, administrative staff, local government, government, representatives of other sectors whose actions also determine health capital. This concept also reveals the spectrum of actions that must be taken for health to be ours, viz: education, prevention, health care, rehabilitation, long-term care. Like any other entity, healthcare facilities have an increasingly visible public image. A positive image of a healthcare facility translates into relationships with patients – and also into attracting new patients. There are indeed many ways to build an image and take care of it.

According to A. Fudali (2024), the four most important pillars of a medical facility's image are:

1. Internet visibility (the practice, hospital or clinic should ensure that it is easy to find on the Internet);
2. staff image and involvement (ensuring good communication and positive feedback about the organisation's staff);
3. accessibility for patients (creation of tools to facilitate access to the facility);
4. patient feedback and experience (attention to positive online reviews of the facility).

The basic aim of public relations activities in a specialist's practice, irrespective of the field he or she represents, should be to create a place that is friendly to both patients and colleagues and to increase awareness of the provider in the local market for medical services and, as a result, to effectively create and maintain a positive image. It can be said that the image of a health care facility is influenced by two groups of factors, viz:

1. personal, the so-called art of personal promotion. The basic instruments of personal promotion of medical services include various means of communication, in particular a smile, tone of voice, choice of words, shaking hands, being escorted to the door after an appointment, etc.;
2. tangible (tangible elements, in particular related to the building/room and its equipment. Among others, the absence of

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

architectural barriers, a nice building façade, clear labelling (information signs), location (e.g. parking and/or location close to bus stops), well-kept surroundings are important for a positive perception of the building).

Health services are primarily based on information. It is above all information that creates trust in whoever is providing the service. This is why all the data available to patients, but also those that constitute the 'content' of public relations activities, play such an important role.

INTERNET PUBLIC RELATIONS IN HEALTH CARE

We can divide the activities related to the promotion of healthcare facilities on the Internet into three main groups: Internal e-PR, media relations i.e. media relations and external e-PR.

Internal activities are the creation of factors that facilitate communication within the organisation – on the web, it is an efficient e-mail or Internet bulletin boards or entire website elements for use by employees. Internal communication is of great importance when it comes to the functioning of any organisation. The same is true in healthcare. Efficient doctor-staff-patient communication channels are also linked to this.

Media relations in our case are online contacts with the media: interviews, press releases, advertisements, sponsored articles, media patronage – generally contacts that are accessible via the Internet or visible there. This department is a field for creativity on the part of healthcare professionals. Depending on the degree of their involvement with the media, this can bring huge advertising benefits for their practices or clinics.

External e-PR is primarily the organisation's website. The design of the website should be preceded by a definition of its purpose and addressee. When deciding to create a website, special attention should be paid to the graphic design of the layout of the individual elements on the site (so-called layout) and the navigation (appropriate and functional arrangement of the elements used to move around the site). The content of the site should be particularly easy to navigate and clearly laid out, given the potentially wide audience (including older people). When setting

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

up the site, it is fundamental to establish the address, which should be obvious, short and easy to remember. If the practice has a logo, this should be included on the site. If not, setting up the site is a good opportunity to design a logo. The logo, or the organisation's logo, reinforces the organisation's identity and helps to distinguish it from competing entities. A website is essentially a web-based business card, so it should be as good as possible and include the following elements:

- the latest information on the facility,
- history of the organisation,
- scope of services,
- health promotion materials,
- health topics (e.g. health advice),
- the organisation's public documents,
- statements and comments on specific events,
- press releases/materials and published in the press, photographs,
- list of frequently asked questions,
- clearly distinguishable address details.

The site should not be purely text-based, but should make full use of the multimedia possibilities of the web, i.e. animation, sound, images, videos. The site should be informative and educational, but also provide a communication channel. The website can also make use of a banner, i.e. an elongated graphic strip and a FAQ option (a list of frequently asked questions with answers). In addition, a subscription option can be created on the practice's website for subscribers who are interested in receiving malaise from a specific area (e.g. changes in appointment times, holidays). The subscription should, of course, be free of charge. It is possible to link it to an electronic survey, e.g. on expectations in terms of availability or type of service. The primary role of the website is to differentiate the practice's offerings from those of its competitors and to build the practice's reputation. In summary, the medical practice should use its website to communicate with patients (existing and potential), inform them about the scope of its services and create a positive image of the organisation.

In addition to the website, the Internet can also be used in creating the image of the organisation, through: the ability to easily contact different units, responding promptly to e-mails, positioning the website in leading search engines, newsletter

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

opportunities, blogs, messaging, advertising, prevention and public health campaigns.

LIMITATIONS OF E-PR IN HEALTH CARE

Medicine is a special field of life. Its purpose is to protect human life and health. Doctors belong to a group of so-called liberal professions, in which the possibility of advertising services is limited both by generally applicable law and by the rules of professional ethics established by professional self-governments. Health care is one of the few fields in which strong legal interference in advertising is apparent. Pursuant to Article 56 of the Act on the Profession of Physician and Dentist, a physician performing individual medical practice or individual specialist medical practice and a group medical practice may make public information about the health services provided. However, the content and form of such information must not have the characteristics of advertising. This regulation coincides with Article 18b of the Act of 30 August 1991 on health care institutions, which means that the law imposes the same restrictions on information made public by both health care institutions (public and non-public) and so-called private medical practices (individual and group). Article 56 (2) of the Act on the professions of physician and dentist, empowers the Supreme Medical Council to determine the rules of making the information in question public. The detailed rules adopted by the doctors' professional self-government on 'advertising' concerning individual practices are contained in Resolution No. 18/98/III of the Supreme Medical Council of 25 April 1998 on detailed rules of publicising information on the provision of health services by doctors within the framework of individual medical practice. Due to legal restrictions on the advertising of health care services, a permitted alternative for health care providers is becoming public relations (*Public relations of the doctor's surgery*).

In addition, every doctor is obliged to respect the rights of the patient in their work, which include:

- the right to consent to health services,
- the right to information about health conditions,
- and the right to respect for dignity and intimacy.

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Every physician should act in accordance with the Code of Medical Ethics, where Article 2 states that "the vocation of a physician is: to protect human life and health, prevent disease, treat the sick and relieve suffering. A doctor may not use medical knowledge and skill in activities contrary to this vocation" (Muszala, 2013). This must also translate into marketing activities concerning health care entities. Permitted marketing activities in medicine must comply with ethical principles and legal regulations. Medical entrepreneurs should only use permitted marketing activities to effectively reach their target group and attract loyal patients. They must avoid activities that are dangerous to patients' health or violate ethical principles. All marketing activities must be based on reliable information. Among the group of activities prohibited by law or contrary to ethics are the following:

- advertising of non-prescription medicines. Advertising of non-prescription medicines is prohibited in some countries. Without consulting a doctor, it can be dangerous and pose a health risk to patients;
- advertising of medical services that are not available. Medical entrepreneurs may not advertise medical services that are not available or that are not performed by a particular medical facility. Such advertising may be misleading and confusing to patients;
- promises of treatment without scientific backing. Medical entities may not promise treatment without scientific backing. Such advertising may mislead patients and violate their rights;
- advertising cosmetic treatments as medical procedures. Medical entities may not advertise cosmetic treatments as medical procedures. Such actions may mislead patients and be dangerous to their health;
- use of well-known public figures in medical advertisements. It is not permitted to use well-known public figures in medical advertisements without their consent. Such actions may mislead patients and violate the privacy of public figures.

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

RISKS ASSOCIATED WITH E-PR IN HEALTH CARE

The use of the Internet in any field gives rise to a variety of threats. The nature of the web means that the data it contains can easily fall into unwanted hands and become the basis for criminal activity. It is no different in the context of healthcare entities. Due to the nature of their activities, they have long been overlooked as a target for hacking attacks. However, the ease of access to patient data held by hospitals or clinics has brought them to the attention of criminals and they are now subject to almost the same risk of attack as banks or government offices. Cybersecurity measures are only just being introduced in many healthcare facilities, which also provides an incentive for hackers. And the number of Internet-related threats continues to grow. Also in the area described: "In Poland in 2023, we had 43 reported hacking attacks on medical facilities. Meanwhile, in 2021, there were only 13 (an increase of more than 300%). Globally, on the other hand, hacking attacks in healthcare are estimated to reach a figure of 1,800 per week (a 74% increase compared to 2022)" (Poradyodo.pl, 2023).

Huge amounts of data are sent through the IT systems of healthcare providers every day, the potential leakage of which has consequences far more serious than just financial. The data that is processed by these systems includes information on diseases, medicines or patients' address data. The possession of such information by cyber criminals, provides them with enormous opportunities, above all they can blackmail healthcare facilities as well as individuals. "Data leaks are very painful for both healthcare facilities and patients, but recently a new, more serious consequence has emerged, namely tampering with the systems of machines used to hospitalise patients. The problem here is that modern medical machines, despite their advanced life-saving systems, are themselves quite susceptible to external interference, including remote interference via a computer network, which may even have the effect of causing death to the patient" (Nawrocki, 2021).

The main dangers of using Internet public relations include:

- phishing (manipulating the user and exploiting his/her trust in order to obtain data or carry out phishing);

- malware (installation of malicious software that can steal data, slow down or damage systems thereby exposing healthcare facilities to loss);
- ransomware (locking up computers, which can make it easier for hackers to access the system while making it difficult for the facility – the victim – to operate);
- DDoS attacks (deliberate overloading of the server which exposes the organisation's activities – victims to downtime, losses);
- privacy risks (illegal use of patient data);
- data theft (*idem*);
- identity theft (*idem*);
- dangerous advertising (advertising as a tool to attack a health care facility);
- spoofing (when a fraudster pretends to be someone else);
- watering hole attacks (attacks against a specific group, site);
- Internet fraud (not everything on the web is real);
- and many others... (bezpiecznyinternet.edu.pl, 2024; Nawrocki, 2021).

As can be seen from the list above, there are two types of risks associated with the use of the Internet in healthcare. The first are those that target the acquisition of information, specifically the theft of patient data. If successful, the fate of the stolen data could be manifold, ranging from selling it to various types of companies to using the stolen identities for criminal purposes. The second type of threats are those that target the healthcare entity and aim to harm it. These may include, for example, acts of unfair competition. For opponents of the introduction of the Internet into healthcare public relations, the large number of threats is the main argument in the discussion, but it seems that this is not a good argument. The Internet is still the tool of the future in almost every area of life. It is no different in the case of medicine in its broadest sense. Its use carries many dangers, but it is important to remember that as they develop, so do the ways and tools that can prevent them. Therefore, a necessary requirement for today's surgeries, clinics or hospitals is to invest not only in PR, but also in cyber-security systems that will help reduce the risk of online activities (Ezdrowie.gov.pl, 2022; Kuchta, 2023).

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

SUMMARY

Public relations in healthcare is an important tool for medical entrepreneurs to help promote medical services and products, attract and retain loyal patients and increase profits. However, it must not violate patients' privacy or mislead them. The use of online public relations techniques and activities is a requirement of the modern age. It is desirable and necessary. It is also beneficial for all parties to this type of communication. Even in spite of the many risks (those online, because ethics and the law must be respected unconditionally), it is worth investing in this type of activity – with appropriate safeguards – not only to move with the times, but above all to act effectively, which in a field such as health care is particularly important. The focus should be on protecting the IT systems and devices used by the health service. That an attack will occur can be almost certain due to the increasing digitalisation and consequent development of cybercrime. Furthermore, the data stored on these servers is very tempting for attackers. Hence, it is very important to make healthcare professionals and patients aware of the existence of such threats, as well as their consequences. Those responsible for the security of healthcare systems face a huge task on the technical side to secure such valuable data, but it is equally important to train each healthcare professional in basic cyber threats so that they know how to respond in the event of an attack.

The web is one of the main sources of health knowledge today. Artificial intelligence can recognise the symptoms of diseases and advise on basic treatments. Teleportation has also become very popular. Patients can move with the times and take advantage of these facilities, but they should not trust what they find online unreservedly.

BIBLIOGRAPHY

Acts:

Act of 5 December 1996 on the professions of physician and dentist (Dz. U. 1997 No. 28 item 152).

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Act of 30 August 1991 on health care institutions (consolidated text: Journal of Laws of 2007, No. 14, item 89, as amended). The Act of 30 August 1991 on health care institutions (consolidated text: Journal of Laws of 2007, No. 14, item 89, as amended).

Resolution No 18/98/III of the Supreme Medical Council of 25 April 1998 on the detailed principles of publishing information on the provision of health services by doctors within the framework of individual medical practice.

Literature:

Cenker, E. M. (2007). *Public relations*.

Dobska, M., & Rogoziński, K. (2008). *Podstawy zarządzania zakładem opieki zdrowotnej*. WN PWN.

Dolczewska-Samela, A. (2008). Significance of the medical staff-patient relationship for the course of the treatment process. In H. D. Głowacka (ed.), *Szanse i bariery w ochronie zdrowia. Selected organisational, legal and psychological aspects*. Wydawnictwo Naukowe Uniwersytetu Medycznego im. K. Marcinkowskiego w Poznaniu.

Golinowska, S., Rutkowska-Czepulis, Z., Sitek, M., Sowa, A., Sowada, Ch., & Włodarczyk, C. (2002). *Opieka zdrowotna w Polsce po reformie*. CASE – Centrum Analiz Społeczno-Ekonomicznych.

Holecki, T., Skrzypek, M., & Szlapa, M. (2013). Shaping the image of the primary health care facility in the context of the role of the family doctor. *Studia Ekonomiczne*.

Hope, E. (2013). *Ethics in the profession of public relations specialists*.

Łazorko, K., & Syrkiewicz-Świtała, M. (2011). Public relations in health care. In M. A. Syrkiewicz-Świtała (ed.), *Marketing in health care* (pp. 79–81).

Maciejowski, T. (2003). *Narzędzia skutecznej promocji w Internecie*.

Pluta, E. (2001). *Public relations – fashion or necessity?: Theory and practice*.

Przybylski, H. (ed.). (2006). *Public relations. Effective communication in theory and practice*.

Rozwadowska, B. (2002). *Public relations: Theory, practice, perspectives*.

Smektała, T. (2006). *Public relations on the Internet*.

Tworzydło, D. (ed.). (2003). *Public relations*. *Materials of the 2nd PR Congress*. Conference Centre of the University of Information Technology and Management in Rzeszów.

Wójcik, K. (2015). *Public relations. Credible dialogue with the environment*.

Online sources:

Anywhere.pl (n.d.). *Health service or health care – which name irritates doctors?* https://anywhere.pl/107884/sluzba-zdrowia-czy-ochrona-zdrowia-ktora-nazwa-drazni-lekarzy/ (14–06–2024).

Bezpiecznyinternet.edu.pl (2024, May 14). *Major online threats: What you need to watch out for.* https://bezpiecznyinternet.edu.pl/glowne-zagrozenia-w-internecie-na-co-musisz-uwazac/ (16–06–2024).

Biedrzycki, N. (2017, April 26). *Medicine of the future, or IT-assisted health.* https://www.forbes.pl/technologie/medycyna-przyszlosci-czyli-informatyczne-wspomaganie-zdrowia/wpr83jp (15–06–2024).

Cieniek, R. (2024, May 17). *Internet and medicine, opportunities and threats*. https://holistic.news/internet-i-medycyna-szanse-oraz-zagrozenia/ (14–06–2024).

De Jong, T., & Bos, E. (2014). *Existing and emerging risks in the healthcare sector, including home care and out-of-hospital care*. European Risk Observatory. Report summary. https://osha.europa.eu/sites/default/files/healthcare%20sector%20-%20pl.pdf (15–06–2024).

Ezdrowie.gov.pl (2022, May 19). *Healthcare Cyber Security Action Plan, E-Health Centre Recommendations for Building Cyber Security Systems Version 1.2*. https://ezdrowie.gov.pl/portal/home/wytyczne-i-rekomendacje-cez/plan-dzialania-w-zakresie-cyberbezpieczenstwa-w-ochronie-zdrowia (16–06–2024).

Fudali, A. (2024, September 24). *4 pillars of a medical facility's image*. https://pro.znanylekarz.pl/blog/placowki/wizerunek-placowki-medycznej (15–06–2024).

Kuchta, P. (2023, June 20). *Cyber security in hospitals – how to protect against hacking attacks*. https://www.poradyodo.pl/cyberbezpieczenstwo/cyberbezpieczenstwo-w-szpitalach-jak-zabezpieczyc-sie-przed-atakami-hakerskimi-12256.html (16–06–2024).

Medical marketing. Permitted and prohibited activities. https://simpliteca.com/medycyna/marketing-medyczny-dozwolone-i-zabronione-dzialania/ (14–06–2024).

Muszala, A. (2023, November 5). *KEL: What is the purpose of medicine*. https://www.mp.pl/etyka/podstawy_etyki_lekarskiej/91334,jaki-jest-cel-medycyny-kodeks-etyki-lekarskiej-odcinek-9 (15–06–2024).

Nawrocki, S. (n.d.). *Cyber threats in the health care sector, including anaesthesiology and emergency medicine. Characteristics of selected threats and ways of prevention*. https://www.akademiamedycyny.pl/wcontent/uploads/2021/10/AiR_2_2021_02.pdf (16–06–2024).

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Nowak, N. (2024, January 9). *Health care or health service?* https://politykazdrowotna.com/artykul/ochrona-zdrowia-czy-sluzba/1211497 (15–06–2024).

Paciorek, E. (2021, October 25). *Towards e-health. Opportunities threats*. https://serwiszoz.pl/prowadzenie-dokumentacji-medycznej/w-kierunku-ezdrowia-szanse-i-zagrozenia-1814.html (15–06–2024).

Politykazdrowotna.com (2022, July 22). *Health care versus service, or the conceptual, and more, dispute between medics and politicians*. https://politykazdrowotna.com/artykul/ochrona-zdrowia-kontra/904377 (15–06–2024).

Poradyodo.pl (2023, 21 November). *Cyber security in hospitals and other medical facilities – more and more hacking attacks*. https://www.poradyodo.pl/ado/cyberbezpieczenstwo-w-szpitalach-i-innych-placowkach-medycznych-coraz-wiecej-atakow-hakerskich-12463.html (16–06–2024).

Prawo.pl (2010, April 9). *Public relations of a specialist doctor's practice*. https://www.prawo.pl/zdrowie/public-relations-gabinetu-lekarza-specjalisty,236900.html (15–06–2024).

Szarkowska, E. (2022, April 7). *Służba zdrowia czy system ochrony zdrowia*. https://nursing.com.pl/artykul/sluzba-zdrowia-czy-system-ochrony-zdrowia-624df163d4b705397165c390 (15–06–2024).

Bichta, S. (2025). E-public relations in healthcare and associated risks.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 163–176). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Paulina Szaniawska

Faculty of Political Science and Journalism of the Maria Curie-Skłodowska University
E-mail: paulina.military02@gmail.com
ORCID: 0009-0009-9421-6307

ETHICS AND SECURITY RELATED TO AI IN MEDICINE

Abstract: Artificial intelligence (AI) in medicine is becoming one of the most important tools to support diagnosis, therapy and management of healthcare systems. However, its rapid development comes with a number of ethical challenges and risks related to related to safety. Key issues include algorithmic biases, medical data privacy, accountability for AI decisions and the availability of these technologies. The article discusses issues related to transparency, inequalities in access to AI, and the impact of these technologies on the doctor-patient relationship. Particular attention is given to regulations that should keep up with the rapid pace of AI implementation in medicine. Potential solutions that can help the sustainable and responsible development of this technology are also proposed.

Keywords: artificial intelligence (AI), medicine, ethics, data security, privacy, transparency.

INTRODUCTION

Artificial intelligence (AI) is defined as the ability of machines to mimic human intellectual processes such as analysis, learning and decision-making. Its rapid development over the past few years has led to its increasing application in in medicine. AI not only assists doctors in diagnosis and treatment, but also sets new standards in the management of medical facilities. However, the introduction of this technology comes with ethical, technological and social challenges that require attention to ensure AI can safely and effectively support the healthcare system.

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Artificial intelligence systems are now being used worldwide in various areas of medicine, such as diagnostics, analysing imaging results and supporting the selection of the most appropriate therapy for patients. Machine learning algorithms also play a key role in developing new drugs, identifying potential therapeutic targets and virtually testing the effectiveness of new molecules.

The COVID-19 pandemic has accelerated the use of AI in public health activities, including health systems management and infectious disease monitoring. These technologies are also being used to preselect patients with suspected SARS-CoV-2 virus infection. In turn, restrictions on social interactions and impeded access to health services have contributed to the growing popularity of combining mobile technologies with AI systems, which are increasingly being used to monitor the health of formally healthy people who want to take an active interest in their wellbeing.

Support from AI algorithms also enables better access to health services for residents in non-urbanised areas and remote from large medical centres, the World Health Organisation reminds. A paper published by the WHO entitled 'Ethics and governance of artificial intelligence for health' (WHO, 2021) indicates that the potential of AI should not be overestimated, especially when the implementation of such technology comes at the expense of investment to universalise access to health care.

Like any innovative technology, artificial intelligence has great potential to significantly improve access to medical services for millions of people around the world. At the same time, like other technologies, it can be misused, leading to harm to people, noted Dr Tedros Adhanom Ghebreyesus (WHO, 2021), Director-General of the World Health Organisation. – This report is a valuable guide for governments that want to maximise the benefits of from the use of AI, while minimising risks and avoiding potential problems.

According to the authors of the WHO report, the document is mainly aimed at public policy makers, such as ministries of health, regulators or legislators, responsible for implementing technology to improve the quality of life of citizens. However, the guidelines and examples it contains can also be a valuable resource for technology companies, scientists, researchers and health professionals.

SIX PRINCIPLES OF WHO

Public and private investment in the development of artificial intelligence technologies is key to improving health services, the report's authors note. However, a lack of adequate regulation in this area could jeopardise the rights of patients and communities, exposing them to commercial efforts by large technology corporations focused on maximising profits. For this reason, the World Health Organisation (WHO) calls for systemic oversight by governments. Such oversight should encompass every stage – from design to implementation to operation of AI systems.

Experts involved by WHO in the development of the report formulated six basic principles that can help in the evaluation and implementation of artificial intelligence in the health sector (WHO, 2021):

1. Protecting human self-determination. Final clinical decisions must belong to humans and not to AI systems. It is crucial to ensure privacy and the protection of medical data, and to obtain informed consent from patients for its use in accordance with applicable regulations.
2. Promoting wellbeing, safety and public interest. Systems for measuring and controlling quality in AI-enabled environments are needed. Algorithm developers should comply with regulations regarding safety and effectiveness in specific medical applications.
3. Transparency and comprehensibility. Information about AI systems should be public and available in a way that it can be understood. A public debate on the use of AI in medicine is essential to build public trust.
4. Promoting accountability. It is crucial to implement control mechanisms to assess the effectiveness of AI and eliminate harm from its use. These technologies should only be used by appropriately trained personnel and within the guidelines set.
5. Ensuring equality and inclusivity. AI algorithms should be designed so that their benefits extend to the widest possible audience, regardless of characteristics such as age, gender, socio-economic status or ethnicity.
6. Promoting sustainability and environmental responsibility. AI systems must be designed to minimise their environmental

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

impact and optimise energy consumption. In addition, stakeholders should take measures to mitigate the effects of automation, such as job reductions, by providing training and support for medical staff adapting to new technologies.

The WHO report points to the need for responsible deployment of AI to maximise the public health benefits while mitigating the risks associated with its use.

APPLICATION OF AI IN MEDICINE

Artificial intelligence (AI) is a technology that is playing an increasingly important role in various areas of life, including medicine. With its ability to process vast amounts of data, learn from it and make decisions, AI is becoming an invaluable support for medical professionals. Since the first attempts to use this technology in diagnostics in the 1960s, AI has come a long way, evolving from simple algorithms to advanced systems based on deep machine learning (CNN) and machine learning (ML) (Medidesk, 2024). Currently, its applications include areas such as medical image analysis, personalisation of therapy, patient monitoring or clinical decision support.

AI is not only increasing the precision of diagnosis and the effectiveness of treatment, but is also revolutionising the daily work of doctors, enabling a more efficient use of time and resources. Despite the huge potential of this technology, its integration into the healthcare system comes with a number of challenges, such as the need to ensure the security of patient data, transparency in decision-making and the creation of appropriate regulations. Nevertheless, AI promises to be a key part of the future of medicine.

1. The first applications of AI in medicine took place as early as the 1960s, but it is only the current technological developments that allow its potential to be put into in practice. Contemporary application examples include (WHO, 2021).
2. Imaging diagnostics: programmes can analyse X-ray images, CT scans and MRI scans, often with a precision that rivals that of specialists.

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

3. Oncology: IBM's Watson assists in the selection of oncology therapy, taking into account individual patient characteristics, which reduces diagnosis time and increases treatment effectiveness.
4. Telemedicine: DeepMind Health has developed Streams, an app that allows real-time monitoring of a patient's health status, making doctors more efficient.

BENEFITS OF AI

The application of artificial intelligence in medicine opens up new possibilities that were previously beyond the reach of traditional diagnostic and therapeutic methods. AI can analyse medical data quickly and accurately, enabling doctors to make more accurate decisions in less time (Medidesk, 2024). With this technology, it is also possible to identify subtle patterns in test results that may be missed by humans. This in turn allows for earlier detection of diseases and more effective treatment of patients.

Additionally, AI can automate many tedious administrative tasks and analytical tasks, relieving the burden on medical staff and allowing them to focus on the individual needs of the patient. The introduction of AI also promotes greater accessibility to healthcare, reducing waiting times for appointments or test results. The benefits of this technology have the potential not only to improve the work of doctors, but also to increase the comfort and safety for patients, making healthcare more efficient and modern.

The introduction of artificial intelligence into medicine brings many benefits such as reduced diagnostic and treatment times, where AI algorithms can process medical data in a fraction of the time needed by a human, increased efficiency of diagnoses thanks to AI's ability to detect subtle changes that can be missed by a human, AI also simulates the development of clinical conditions, enabling precise treatment planning, but also helps to automate administrative processes and analytical processes, allowing doctors to focus on patients (WHO, 2021). With these advantages, AI can help to improve the quality of medical services, as well as reduce the operational costs of healthcare facilities.

ETHICAL AND SOCIAL CHALLENGES

The development of artificial intelligence (AI) in medicine is generating not only excitement about the of the potential benefits, but also deep reflection on the ethical and social implications of its implementation. As a technology capable of autonomously analysing data, making decisions and predicting clinical outcomes, AI raises questions about the limits of its responsibility, its impact on the doctor-patient relationship and the transformation of professional roles in the medical sector. These dilemmas are particularly relevant in the context of the complexity and unpredictability of clinical processes, where every decision can have a direct impact on patients' lives and health.

One of the key ethical challenges is the problem of the so-called 'black box', or lack of transparency in the operation of AI algorithms. Although the technology can achieve impressive results in diagnosis and treatment, the decision-making processes on which AI is based often remain incomprehensible to users – including doctors. This causes difficulties in assessing the reliability of results and limits the ability of specialists to control the system's work. This raises the question of responsibility for possible AI errors: should it be borne by the algorithm developer, the supervising physician, or perhaps the medical facility that decided to implement the technology?

Another issue is the impact of AI on human relationships in medicine. Patients often stress the importance of empathy and the doctor's involvement in the treatment process – values that are difficult to replace with technology. The automation of some aspects of medical work, while streamlining many processes, runs the risk of objectifying the patient, which can lead to a loss of trust in the healthcare system. At the same time, AI is changing the way professional roles in medicine are perceived. Concerns about automation and the replacement of humans by machines are causing anxiety among doctors and medical students who fear losing their jobs or marginalising their role.

There is also the issue of data security. Artificial intelligence requires the processing of huge amounts of sensitive medical information, which poses the risk of privacy breaches and

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

unauthorised access to patient data. With the popularisation of AI, it becomes necessary to develop rigorous data protection standards and encryption methods to prevent misuse (Medidesk, 2024). The potential impact of AI on medical education and professional practice is also not insignificant. There is a risk that over-reliance on technology may lead to the disappearance of some key skills, such as physical examination and intuitive clinical decision-making. In the long term, this could reduce the competence of future generations of doctors, who will depend more on technology than on their own knowledge and experience.

These and other societal and ethical challenges require comprehensive analysis and appropriate action. It will be crucial to develop clear regulations that define the rules for the use of AI in medicine (WHO, 2021), and the creation of educational systems that prepare both doctors and patients to cooperate with this technology. The development of artificial intelligence carries enormous potential, but its effective and safe use requires a thoughtful approach that takes into account the needs of both patients and and medical staff.

POTENTIAL RISKS AND BARRIERS

Artificial intelligence (AI) in medicine raises great hopes but, at the same time, is a source of major concerns and challenges. Despite its enormous technological potential, the implementation of AI faces various barriers and poses significant risks that could affect both patients and healthcare systems. The adoption of this technology requires not only advanced technical solutions, but also a rethinking of legal, ethical and organisational issues that can significantly affect the effectiveness and safety of its use.

One of the most commonly cited risks is the potential for AI systems to make diagnostic and therapeutic errors. While algorithms can achieve a high level of efficiency in analysing medical data, their decisions are based on patterns in available databases. If this data is incomplete, inaccurate or subject to errors, AI can draw misleading conclusions. This can lead to serious health consequences, especially in situations where time and precision are of the essence, such as emergencies.

Another barrier is the 'black box effect' (Grace *et al*., 2018), i.e. the lack of transparency in how AI systems make decisions. Even for their creators, it is often difficult to explain exactly on what basis an algorithm has reached a particular conclusion. This lack of understanding can create distrust among doctors and patients, and make it difficult to assess the correctness of the system. As a result, the question arises as to who should be responsible for the consequences of any errors – the technology developer, the medical facility or the supervising physician.

The high cost of implementing artificial intelligence is also not insignificant. The purchase of equipment, the creation of the relevant algorithms and the training of staff all require significant financial resources, which limits the availability of this technology, especially in smaller facilities or countries with limited healthcare budgets. Furthermore, the integration of new technological solutions involves a lengthy testing and implementation process, further increasing costs and adaptation time.

From a societal perspective, resistance from medical staff is also a significant challenge. Many doctors fear that artificial intelligence could replace them in their day-to-day duties, which could lead to a reduction in demand for certain specialties, such as radiology or pathomorphology. Such fears, although often unfounded in the short term, can negatively affect the willingness of staff to use the technology.

The issue of data security cannot be overlooked either. AI requires the processing of vast amounts of sensitive medical information, which poses risks to patient privacy and the possibility of unauthorised access to data. Developing effective methods to secure this information is a priority, but even the best systems can be vulnerable to cyber-attacks.

The implementation of artificial intelligence in medicine is a complex process and multifaceted. In order to avoid potential risks and overcome existing barriers, extensive measures are required, such as creating regulations, investing in staff education and ensuring data security. Only the combination of these elements will allow AI to be used to its full potential in a safe and responsible manner.

THE FUTURE OF AI IN MEDICINE

Artificial intelligence (AI) in medicine is on the threshold of a disruptive change that has the potential to change healthcare delivery forever. Advances in technology and the increasing availability of medical data are enabling increasingly sophisticated applications of AI, from diagnosing diseases to personalising treatments and managing processes in medical facilities (Kaplan & Haenlein, 2019, pp. 15–25.). As the technology develops, it is becoming clear that its impact on medicine goes far beyond the current framework, offering entirely new opportunities to improve the quality and efficiency of treatment.

In the coming years, AI has the potential to become an integral part of healthcare systems (Grace *et al.*, 2018, p. 62). Algorithms based on machine learning and deep neural networks will not only be able to analyse test results faster and more accurately than humans, but also predict disease risk based on genetic and environmental data. This approach will enable even more effective disease prevention, the development of personalised treatment plans and the minimisation of the risk of complications.

The future of AI in medicine also includes the development of technologies to support the daily work of doctors. AI-enabled intelligent medical decision support systems, surgical robots or telemedicine platforms can not only ease the burden on medical staff, but also increase the availability of healthcare in regions where there is a shortage of specialists. What's more, virtual medical assistants can help patients monitor their health and remind them to take their medication, increasing patient engagement in the treatment process.

However, the future of AI in medicine is not just about promises. The implementation of these technologies will require addressing a number of challenges, such as ensuring the transparency of algorithms, the protection of patient data, and regulations that balance the development of technology with an ethical approach to healthcare (Khan *et al.*, 2017, pp. 8–13). Also key will be a change in the education of future doctors, who will need to learn how to work effectively with AI-based systems.

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

While there is still a long way to go before AI is fully integrated into medical systems, the possibilities that this technology brings are inspiring. If implemented thoughtfully and ethically, it can contribute to a healthcare system that is more precise, accessible and patient-centric than ever before.

SUMMARY

Artificial intelligence (AI) is one of the fastest growing areas of technology that has the potential to revolutionise medicine on many levels. Its ability to process vast amounts of data, learn from it and make real-time decisions is opening up new possibilities in diagnosis, therapy and healthcare management. The use of AI, from analysing medical images to personalising treatment and assisting surgery, is already bringing tangible benefits such as more effective diagnoses, faster implementation of treatments and easing the burden on medical staff.

However, the development of AI in medicine also brings with it numerous challenges and potential risks. Issues such as the lack of transparency of algorithms, data security or liability for diagnostic errors require special attention. Ensuring appropriate regulation and education of medical personnel so that the technology can be used ethically and safe.

The future of AI in medicine seems promising, but its full exploitation requires a balanced approach that combines advanced technological capabilities with empathy and human experience. Only a harmonious collaboration between doctors and AI systems will allow the creation of an effective and sustainable healthcare model that serves both patients and society as a whole. Introducing AI into medicine is a complex and challenging process, but its potential benefits can significantly outweigh the challenges if done thoughtfully and responsibly.

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

BIBLIOGRAPHY

Grace, K., Salvatier, J., Dafoe, A., Zhang, B., & Evans, O. (2018). When will AI exceed human performance? Evidence from AI experts. *Journal of Artificial Intelligence Research*, *62*, 729–754.

Kaplan, A., & Haenlein, M. (2019). Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Khan, O., Comm, B., Bebb, G., & Alimohamed, N. A. (2017). Artificial intelligence in medicine – What oncologists need to know about its potential and its limitations. *Oncology Exchange*, *16*(4), 8–13.

Medidesk, M. (2024). *Ethical aspects of the use of artificial intelligence in medicine*. https://medidesk.pl/etyczne-aspekty-stosowania-sztucznej-inteligencji-w-medycynie/ (15-11-2024).

WHO (2021.) *Ethics and governance of artificial intelligence for health*. https://www.who.int/publications/i/item/9789240029200 (15-11-2024).

Szaniawska, P. (2025). Ethics and security related to AI in medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 177–187). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Źródło: Wydawnictwo Academicon / Academicon Press

Aleksandra Kramek

Faculty of Political Science and Journalism, Maria Curie-Skłodowska University
E-mail: kramekola@wp.pl
ORCID: https://orcid.org/0009-0005-0790-017X

AI IN MODERN MEDICINE

Abstract: Artificial intelligence (AI) is becoming a key component of modern medicine, revolutionising the way we diagnose, treat and monitor patients' health. This article discusses the most important applications of AI in different areas of medicine, such as mental health support, telemedicine and chronic care. It highlights how machine learning algorithms support physicians in fast and accurate decision-making, as well as how mobile apps and smart devices help patients in their daily health management. It also addresses the ethical issues and challenges of implementing AI in medicine, including the protection of patient data and the transparency of system operations. The article points out that the development of AI in medicine not only improves the quality of healthcare, but also opens up new possibilities in the diagnosis and treatment of diseases that were previously difficult to control.

Keywords: artificial intelligence, medicine, mental health, ethics, telemedicine.

INTRODUCTION

Artificial intelligence (AI) is playing an increasingly important role in shaping modern medicine, offering innovative solutions that are revolutionising healthcare. From supporting diagnosis and treatment to improving patients' quality of life, AI's possibilities seem almost limitless, but it continues to be an unfamiliar field of endeavour and needs to be looked at heavily, especially in the medical field. Among the key applications, assistance in the area of mental health stands out, where AI

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

supports diagnosis and therapy, especially in times of increasing incidence of depression and anxiety disorders.

Equally important are AI solutions in telemedicine, enabling access to healthcare remotely, which is changing the way patients and doctors communicate on a daily basis. Another important area is the support of patients with chronic diseases – AI monitors their health status and helps to adapt treatment in real time. However, the development of this technology also brings major challenges, especially in the context of ethical issues such as the protection of patient data, the transparency of algorithm performance and the accountability of decisions made by AI systems.

Artificial intelligence is not only changing the way we diagnose and treat patients, it is also raising questions about the future of healthcare and the limits of technology. Thanks to AI, it is possible to analyse huge datasets faster, opening up new possibilities in precise diagnosis, creating personalised therapies or monitoring patients' health at every stage of treatment. However, like any new technology, AI in medicine also raises concerns about its impact on privacy, equity in access to medical services and the ethical aspects of medical decision-making by algorithms. Therefore, although AI has the potential to significantly improve the quality of healthcare, a responsible and thoughtful implementation that considers both benefits and risks is necessary. Those using it should be aware that it is a technology that everyone is learning and should be cautious about.

The development of AI in medicine is not only a technological innovation, but also a profound change in the approach to healthcare. AI makes it possible to create more personalised treatments, reduce waiting times for diagnosis and increase the availability of medical services, especially in regions with limited access to specialist doctors. Thanks to learning algorithms, AI is able to analyse vast amounts of medical data, drawing conclusions that may elude human experts. At the same time, such a dynamic development requires constant reflection on how to combine technological advances with the need to maintain patients' trust and respect their rights. In the following sections of this article, we will look in detail at the applications of AI in mental health, telemedicine, chronic disease management, and discuss the ethical challenges associated with these innovations.

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

This article will discuss these key aspects, showing both the potential and limitations of artificial intelligence in modern medicine. Can AI really be the answer to the challenges of modern healthcare, or does it pose new dilemmas?

AI IN SUPPORT OF MENTAL HEALTH

Artificial intelligence (AI) is playing an increasingly important role in supporting mental health, offering tools that help both patients and professionals. Thanks to advanced algorithms, it is possible to detect mental disorders early, create personalised treatment plans and even intervene in crisis situations.

DIAGNOSIS AND EARLY DETECTION

One of the most important applications of AI in mental health is diagnosing mental disorders at an early stage. Machine learning algorithms analyse data from a variety of sources, such as survey results, posts on online forums or the way patients speak. Natural language processing (NLP)-based technologies allow the assessment of emotional state based on text or speech, which can be particularly useful in identifying depression, anxiety or other mood disorders. Virtual therapists and chatbots, such as Woebot or Wysa, which offer therapeutic support, are growing in popularity. These AI-based tools can conduct therapeutic conversations, suggest stress management techniques or offer relaxation exercises. Their greatest advantage is their accessibility – they can be used at any time, making them particularly helpful for people who do not have the option of traditional psychotherapy. AI also supports the treatment process by creating personalised treatment plans. Analysis of data, such as the patient's treatment history or reactions to previous therapies, allows the appropriate therapeutic and pharmacological methods to be tailored. By continuously monitoring the patient's condition, AI systems can modify recommendations in real time, increasing the effectiveness of treatment. Smart devices such as smartwatches or mobile apps are increasingly being used to monitor the user's

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

mental health. Analysis of sleep patterns, physical activity levels or heart rate can provide valuable information about emotional state and potential risks. This data is then analysed by algorithms that can alert the user or their doctor to take action.

SUPPORT IN CRISIS SITUATIONS

AI plays an important role in the immediate recognition of signals indicating mental health crises, such as suicidal thoughts. AI systems, integrated into support lines, can quickly identify those in need of help and inform the relevant services. This significantly reduces the response time to crises. Although AI offers many benefits, its implementation in the mental health field comes with challenges. One of the most important is the protection of patients' privacy and the security of their data. Systems need to be transparent in order to instil trust in users, and automation cannot replace human contact, which is a key element of psychological therapy (Topol, 2019). Developments in AI are opening up new possibilities for mental health support. In the future, we can expect to see more advanced NLP models and hybrid forms of therapy that combine traditional approaches with AI technologies. This will make psychological support more accessible and effective, especially in cases where rapid intervention can save lives. AI not only supports professionals in their work, but also enables patients to actively manage their mental health, a step towards more holistic healthcare (Naslund *et al.*, 2016; Torous *et al.*, 2020).

AI IN TELEMEDICINE

Artificial intelligence (AI) is changing the face of telemedicine, making healthcare more accessible, efficient and personalised. Through the use of AI algorithms, telemedicine is becoming not only a tool for remote consultations, but also a support for patient diagnosis, monitoring and health management. AI plays a key role in analysing medical data sent by patients. These systems can pre-diagnose diseases based on reported symptoms or test

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

results, allowing doctors to make faster decisions. For example, algorithms that analyse medical images, such as dermatological photos or X-ray scans, help to make an accurate diagnosis, even in a remote care model.

REAL-TIME HEALTH MONITORING

AI systems can assess the urgency of patient requests, automatically classifying cases that require immediate intervention from those that are less urgent. Such solutions not only improve doctors' workflow, but also reduce patients' waiting times for consultation, increasing the efficiency of the entire healthcare system. AI integrates with wearables, enabling the monitoring of health parameters such as blood pressure, heart rate or glucose levels. This data is sent to telemedicine platforms, where AI algorithms analyse it in real time, detecting potential risks and generating alerts for patients and doctors. This makes it possible to react quickly to changes in a patient's condition, especially in the case of chronic diseases.

MANAGEMENT OF CHRONIC DISEASES

AI plays a key role in telemedicine, especially in managing the care of patients with chronic diseases such as diabetes, asthma or hypertension. Advanced algorithms make it possible to tailor treatment plans to individual patients based on analysis of medical data, such as blood glucose levels, blood pressure values or respiratory test results. The systems are able to generate reminders for regular medication intake, minimising the risk of missed doses, and provide patients with detailed instructions on treatment recommendations. By integrating with wearable devices such as smart bands or glucometers, AI monitors health parameters in real time, automatically detecting potential risks, such as rapid drops in blood sugar. If an abnormality is detected, the system can immediately notify both the patient and their doctor, allowing for a quick response and reducing the risk of complications. In addition, AI provides doctors with detailed

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

reports including real-time data collected and historical analysis, making it much easier to monitor the progress of treatment and make any adjustments. This makes it possible to adapt therapies more precisely to the changing needs of patients and to better predict the course of the disease (European Commission, 2021). Through the use of AI in telemedicine, care becomes more comprehensive and personalised, and patients gain a greater sense of security and support in the daily management of their disease.

PERSONALISATION OF HEALTHCARE

By analysing medical data, AI can provide personalised health recommendations. For example, algorithms that predict the risk of developing specific diseases based on a patient's history allow early implementation of preventive measures. This approach increases the efficiency of healthcare and reduces the risk of serious complications. In regions poorly supplied with medical services, AI in telemedicine plays a special role. These tools enable remote consultations that, combined with AI diagnostic support, allow doctors to interpret test results and make decisions without the patient having to be physically present. This is particularly important in remote regions or emergency situations (Jiang *et al.*, 2017).

CHALLENGES, ETHICAL ASPECTS AND THE FUTURE OF AI IN TELEMEDICINE

The implementation of AI in telemedicine comes with some challenges, especially in the context of patient data protection. The storage and analysis of sensitive data must comply with regulations, and AI systems should operate transparently, instilling trust in patients and doctors. It is also crucial to ensure that automation does not completely replace human-to-human contact, which is still an essential part of healthcare. Developments in AI technology are opening up new opportunities in telemedicine. We can expect to see the integration of advanced predictive models to further support patient diagnosis and monitoring.

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Further development of algorithms and tools, such as virtual reality in rehabilitation, will broaden the range of services offered remotely, making telemedicine more comprehensive and efficient. Artificial intelligence in telemedicine not only makes healthcare more accessible, but also allows it to be more precise and personalised, a step forward in modern medicine (American Medical Association, 2022; McKinsey & Company, 2021).

ETHICAL ISSUES AND AI

While the development of artificial intelligence (AI) brings enormous benefits in many fields, it also raises important ethical questions. These issues arise from the dynamic pace of implementation of new technologies and their potential impact on social, economic and cultural life. The following section discusses the key ethical challenges associated with AI. One of the most important ethical issues is that of user privacy and data security. AI often uses huge datasets that may contain sensitive information, for example medical or financial. Ensuring compliance with data protection regulations, such as RODO, and minimising the risk of leaks or unauthorised access remains an issue. The challenge for AI system designers is to simultaneously ensure the effectiveness of the algorithms and the protection of user privacy. AI often acts as a so-called 'black box' – the decision-making processes of algorithms can sometimes be difficult to understand even for their creators. In fields such as medicine or law, there is a need to ensure that decisions made by AI are transparent and verifiable. The lack of such clarification can lead to a loss of trust in AI systems and limit their social acceptance. AI algorithms learn from existing data, which may contain hidden biases and inequalities. As a result, AI can reproduce or even reinforce discrimination in areas such as recruitment, credit allocation or access to public services. The solution is to create more diverse and representative datasets and monitor the performance of algorithms for equality and fairness.

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

AUTONOMY AND RESPONSIBILITY

A major problem is the attribution of responsibility for AI actions, especially in situations where errors occur. In medicine, an algorithm error can lead to a misdiagnosis, and in transport, autonomous vehicles can cause accidents. The question is: who is responsible – the software developer, the user or the organisation implementing the system? Regulatory developments in this area are needed to dispel doubts and ensure consumer protection. Automation and the implementation of AI may lead to job losses in many sectors, raising concerns about the future of employment. Furthermore, in areas such as medicine or education, there is a risk that over-reliance on technology will reduce the importance of human relationships. There is a need to strike a balance between technological efficiency and maintaining a humanistic approach to services. AI is being used to create deepfakes and spread disinformation, affecting public opinion and democratic processes. The manipulation of data and digital content risks destabilising society and undermining trust in the media and public institutions. In this context, it is crucial to develop tools to detect fake content and regulations to counter its spread. AI technologies are often expensive and require sophisticated infrastructure, making access to them uneven. Developing countries may be limited in their ability to benefit from innovative solutions, exacerbating global inequalities. In order for AI to be a tool to support the development of society as a whole, strategies need to be put in place to enable equal access to these technologies. AI developers should be guided by ethical principles when designing systems, taking into account values such as fairness, user welfare and sustainability. In the long term, there is also the question of the potential awareness of AI and its legal status. Could AI in the future be recognised as an autonomous entity with its own rights?

SUMMARY

Artificial intelligence is significantly supporting the development of telemedicine, bringing innovative solutions to the management

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

of patient care, especially for those with chronic diseases. Thanks to advanced algorithms, AI enables the individualisation of treatment plans, real-time monitoring of health status and automatic response to potential risks, such as dangerous changes in vital signs. The integration of AI with wearable devices, such as smart wristbands or glucometers, allows the collection and analysis of medical data, which is then made available to both patients and doctors. This facilitates regular health monitoring, reminds patients to take their medication and provides doctors with detailed reports, supporting them in making sound therapeutic decisions. The use of AI in telemedicine improves the quality of healthcare, increases treatment efficiency and helps to better manage chronic diseases. Patients benefit from more personalised and safer care, and doctors have tools to support them in their work. The development of AI-based technologies in telemedicine shows great potential for further innovations to revolutionise healthcare even further around the world. AI in telemedicine also contributes to improving access to healthcare, especially in regions with limited specialists. With remote monitoring and online consultations, patients can receive regular medical support without frequent visits to facilities. This is particularly important for elderly people, who often have difficulty moving, and patients living in remote areas. In addition, artificial intelligence makes it possible to predict potential health problems based on data analysis, allowing preventive measures to be implemented. As a result, patients with chronic diseases can avoid exacerbations of their conditions and doctors are able to manage treatment more efficiently. This approach significantly reduces the burden on healthcare systems, minimising the need for hospitalisation and emergency interventions. AI-based solutions also support patient education by providing personalised recommendations on lifestyle, diet or physical activity. This facilitates a better understanding of one's disease and greater involvement in the treatment process. Furthermore, AI helps identify high-risk patients, allowing them to be referred for more intensive care before serious health complications arise. In conclusion, AI is not only revolutionising telemedicine, but also contributing to the overall efficiency of the healthcare system. However, its development poses challenges in terms

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

of data privacy, regulation and ensuring equal access to the technology. Nonetheless, the potential of AI in telemedicine remains extremely promising, opening up new opportunities for both patients and medical staff.

BIBLIOGRAPHY

American Medical Association (AMA) (2022). *Ethical Implications of AI in Telemedicine*.

European Commission (2021). *Artificial Intelligence in Healthcare: Telemedicine Applications*.

Firth, J., Torous, J., & Yung, A. R. (2019). Ecological momentary assessment and beyond: The rising interest in e-mental health research. *Journal of Psychiatric Research, 115*, 1–7.

Jiang, F., Jiang, Y., Zhi, H., et al. (2017). Artificial Intelligence in Healthcare: Past, Present, and Future. *Stroke and Vascular Neurology, 2*(4), 230–243.

McKinsey & Company (2021). *Telemedicine and AI: Driving Innovation in Healthcare Delivery*.

Naslund, J. A., Aschbrenner, K. A., Marsch, L. A., & Bartels, S. J. (2016). The future of mental health care: Peer-to-peer support and social media. *Epidemiology and Psychiatric Sciences, 25*(2), 113–122.

Shatte, A. B. R., Hutchinson, D. M., & Teague, S. J. (2019). Machine learning in mental health: A scoping review of methods and applications. *Psychological Medicine, 49*(9), 1426–1448.

Topol, E. J. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books.

Torous, J., Lipschitz, J., Ng, M., & Firth, J. (2020). Dropout rates in clinical trials of smartphone apps for depressive symptoms: A systematic review and meta-analysis. *Journal of Affective Disorders, 263*, 413–419.

Woebot Health (2023). *Evidence-Based Mental Health Support with AI*.

Wysa (n.d.). *AI-Powered Mental Health Chatbot*.

Kramek, A. (2025). AI in modern medicine.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 189–198). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Źródło: Wydawnictwo Academicon / Academicon Press

Łukasz Potocki

Institute of National Security
Faculty of Social Sciences and Humanities, Zamojska Academy
E-mail: lukasz.potocki@akademiazamojska.edu.pl
ORCID: https://orcid.org/0000-0003-3458-1272

REVIEW OF THE POST-CONFERENCE MONOGRAPH

Abstract: This monograph is the result of the 2nd National Scientific Conference on Health Security and Cyberinnovation in Health Care, organized by a consortium of Polish academic institutions. It presents a multidisciplinary perspective on the challenges and transformations occurring at the intersection of public health, national security, and digital innovation, particularly in the aftermath of the COVID-19 pandemic. The publication explores health security as an evolving concept shaped by globalisation, systemic vulnerabilities, and the rapid development of disruptive technologies. The contributing authors address a broad spectrum of topics, including the theoretical foundations of health security, the impact of digitalisation on healthcare systems, the ethical and legal implications of artificial intelligence in medicine, and the societal response to innovations such as COVID passports and telemedicine. The monograph also highlights cybersecurity risks related to patient data protection and public communication in healthcare. Through case studies and conceptual analyses, the volume offers valuable insights into the transformation of health governance under the influence of emerging technologies, and it provides recommendations for the safe and effective integration of cyberinnovation in health systems. The diversity of disciplines and institutional backgrounds of the contributors underscores the complexity and urgency of the issues discussed.

Keywords: health security, cyberinnovation, COVID-19 pandemic, telemedicine, artificial intelligence in healthcare, digital transformation.

The monograph is the aftermath of the 2nd National Scientific Conference on Health Security and Cyberinnovation in Health

Potocki, Ł. (2025). Review of the post-conference monograph.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 199–202). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Care. The event was organised by various academic centres: the Department of International Security of the Institute of International Relations of the Maria Curie-Skłodowska University, the Department of International Political Relations of the Institute of International Relations of the Maria Curie-Skłodowska University, the Department of Visual Communication and New Media of the Institute of Journalism and Management at the Catholic University of Lublin, the 16th Commission on Politics and International Relations of the Lublin Branch of the Polish Academy of Sciences and the International Research Foundation.

The research area of the publication is highly relevant in the context of the current dynamic changes in the international environment. The Covid-19 pandemic has contributed to the consideration of health security as one of the key categories of national security. The increase in the importance of health security threats with its consequences for national and international security has also increased interest and intensified research on this issue which is evident in the topics covered during the conference. It is necessary to refer to the second part of the conference theme, the aftermath of which is a publication. Cyberinnovation and the dynamic development of digital technologies are changing reality in a revolutionary way, and the medical industry is one in which we can expect disruptive innovations. At the same time, it should be borne in mind that the application of new technologies irresistibly involves risks of various kinds, as the authors of the monograph texts point out.

The authors of the texts refer to various issues related to the problem of health safety. In the monograph we have reference to the theoretical and doctrinal perspective of health threats, the concept of combating and neutralising them, and the implications of threats on the contemporary shape of the international environment, including systemic solutions at the international level and selected nation states. The spectrum of issues related to the impact of health threats on various spheres of life of states, organisations and societies is enormous. Undoubtedly, there is also a link between health security and the technological transformation of the modern world, which creates the need to redefine existing models of medical care, data management or public health protection. The articles clearly indicate that modern health systems must incorporate innovative solutions such as artificial intelligence (AI), the Internet of Things (IoT), blockchain or telemedicine technologies.

It should also be emphasised that the authors of the articles represent different research centres and different scientific disciplines which is conducive to solving the research problem.

Marek Pietraś article provides a comprehensive theoretical and doctrinal account of health security. The author of the text classifies health security as a second-generation security dimension, conditioned by globalisation processes, using analytical constructs such as the assumptions of the Copenhagen School and mechanisms of securitisation of the main security dimensions and sectors. Health security thus belongs to the generation of non-military security dimensions conditioned by the processes of globalisation and global mobility.

In her article, Katarzyna Marzęda-Młynarska refers to the category of food security and identifies the challenges facing international food systems after the Covid-19 experience. The threats revealed by the pandemic created the need for changes in the global food system. The author explains precisely how the Covid-19 pandemic affected food security, what were the direct impacts of the pandemic on the different dimensions of security and what might be the long-term consequences of the pandemic for food security and its policies taking into account the impact of technological innovations in the field.

Articles by Małgorzata Gruchoła, Paulina Szaniawska and Aleksandra Kramek address the issue of artificial intelligence (AI) in contemporary healthcare systems. The authors of the texts analyse both the possibility of applying AI in various fields of medicine, such as telemedicine, care of chronically ill patients, mental health treatment (Aleksandra Kramek), as well as addressing ethical and patient safety issues in relation to the use of AI in medicine. In the articles, reference will be made to legal regulations related to the use of artificial intelligence, in which case the problem is keeping up with legal solutions to the rapid advances in AI.

Some articles address the direct effects of the Covid-19 pandemic and its impact on the adopted systemic solutions related to medicine and health care. Justyna Szulich Kałuża and

Potocki, Ł. (2025). Review of the post-conference monograph.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 199–202). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257

Małgorzata Sławek-Czochra create a case study on Covidian passports by analysing, on the basis of empirical research, how Covidian passports were perceived by Polish and EU citizens and whether they are an element of normalisation or are intended to change citizens' behaviour as a behavioural intervention. In turn, Justyna Kięczkowska and Liliana Węgrzyn-Odzioba in their article analyse what challenges and risks the teleportation service poses and provide recommendations to minimise risks in relation to the adoption of new IT solutions in medicine and healthcare. The theme of digitisation is directly addressed in the second text by the above-mentioned authors, in which the process of digitisation of medical services is presented in detail and the security of medical data is illustrated, including the patient's 'personal data'. The security of patient data is also dealt with in his article by Mateusz Wójcik. In Sławomir Bichta's article, in turn, we can find a reference to the media studies sphere. The author focuses on public relations activities in health care and the associated risks. Health care entities are primarily threatened by content presented on the Internet.

The article by Tomasz Bichta is also worth noting. The author undertakes an analysis of a not very popular area in the subject context, which is Angola's health security. Nevertheless, the way in which the health security of this country is presented is interesting both in legal and institutional terms.

In conclusion, the post-conference monograph is a very interesting study. It makes an important contribution to health security research especially in the context of modern technology and innovation. The original approach to the research problem is a valuable addition to the Polish literature in this thematic area.

Potocki, Ł. (2025). Review of the post-conference monograph.
In: Marzęda-Młynarska, K., Węgrzyn-Odzioba, L., Wójciszyn-Wasil, A., Kięczkowska, J. (eds). (2025). *Health security and cyber innovations in health care* (pp. 199–202). Wydawnictwo Academicon. https://doi.org/10.52097/acapress.9788367833257