Targeting the Human Factor: OSINT in Healthcare

Marie Soukupova
Department of Informatics, Faculty of Business and Management, Brno University of Technology, Brno, Czech Republic

Marie.Soukupova1@vut.cz

Abstract: Patients increasingly report that physicians spend more time on the computer than on their examination. While digitalisation is a necessary development in healthcare, it unfolds in a sector constrained by shortages of medical and administrative staff, outdated software and technical infrastructure within the facilities, and uneven levels of digital literacy of medical staff, with the vision of fully paperless healthcare still largely unrealised. At the same time, healthcare has become a target of frequent and sophisticated cyberattacks. In the attempts of a data-driven society, healthcare faces growing demands for efficiency of care provided, interoperability, and timely access to patient data through eHealth solutions. The adoption of emerging technologies, including diagnostic LLMs, is often initiated by medical professionals, sometimes without supervision of IT departments or security teams. As a result, digital transformation increasingly relies on healthcare staff who embrace expanded operational, managerial, and digital responsibilities. This evolution significantly increases the human digital footprint of healthcare professionals and broadens the potential attack surface. As an essential sector under current cybersecurity frameworks, healthcare operates across both professional and private cyberspace. While cybersecurity measures may be implemented by employers during working hours, responsibility for security in private contexts largely depends on individual healthcare workers. Open-Source Intelligence (OSINT) techniques can exploit publicly available data related to professional tasks, online behaviour, and leisure activities, often revealing sensitive insights into clinical practices and personal routines of healthcare staff. From a cybersecurity perspective, healthcare can be perceived as a supply chain in which general practitioners frequently serve as the first point of contact. Due to their limited technical and financial resources, they may represent a structurally vulnerable link within this chain. Although cyber incidents affecting large hospitals attract greater media attention, smaller healthcare providers experience similar threats, which—given the interoperability vision—can have severe implications for the broader healthcare chain. This paper therefore examines OSINT-based human targeting of general practitioners and discusses how information obtained can be leveraged in cyber operations against the healthcare sector.

Keywords: Healthcare, Cybersecurity, OSINT, General practitioners, Supply chain

1. Introduction

When identifying the most important part of CIA Triad (Confidentiality, Integrity, Availability) (Tikanmäki et al., 2025) in the context of healthcare, the crucial one for the essential functions of the system is availability since the medical staff is trained to draw conclusions and further investigate an incomplete documentation rather than work with none or cope with leaked documentation on the way. Furthermore, the healthcare professionals need the documentation to be available as quickly as possible (Tampu & Berek, 2025) since moments have the power to determine the continuation of human life and recovery.

1.1 OSINT

1.1.1 Methodology

The OSINT technique defined as “Open Source Intelligence” is used to analyze publicly accessible and available information in order to gather insights on specific activities or stakeholder groups (Bracciale et al., 2023). Within this technique, the methodology of firstly identifying the target group (in this case, the general practitioners), secondly identifying the main data streams and various dataset sources (this time, namely national registries and statistics office as well as government data and none the less consulting with specialists in health IT and healthcare professionals), information processing and analysis (Bracciale et al., 2023) were the steps involved in the OSINT process.

Firstly, the following steps led to identifying the target group: while hospitals are commonly highlighted by the media as victims of cyberattacks, the publicity of these attacks does not only reflect the frequency and severity of attacks on hospitals as opposed to attacks on different (smaller) parts of the healthcare system as it also considers the appeal of the topic to the general public since the larger the healthcare facility is, the more attention it draws by influencing more patients. However, this fact does not convey that there are no attacks on the smaller parts of the healthcare system (such as GPs). Furthermore, the smaller healthcare facilities function as parts of the supply chain of the hospitals therefore attacks on them suggest consequent implications for the hospitals as well.

While debating the most suitable target group with cybersecurity professionals within the hospitals as part of the research, plenty identified the GPs as most in need of guidance and support since hospitals can allocate a larger range of resources to address cybersecurity challenges compared to the GPs through possibilities of EU/government funding in the form of cybersecurity grants and are more appealing employers to cybersecurity professionals than smaller healthcare facilities. At length, GPs face increasingly limited resources compared to hospitals which implies the necessity to focus on this particular target group within the research.

Secondly, identifying the main data streams and various dataset sources implied focusing on specifically Czech internet within this research considering that healthcare systems around Europe (let alone the globe) vary significantly when it comes to the distribution of care and resources aligned with it. For that reason, considering international sources would not benefit this research. The majority of healthcare in the Czech Republic is coordinated through public health insurance companies that are funded by the state budget and charged by the healthcare facilities per medical performance. Therefore, national registries and statistics together with the ministry of healthcare and websites of GPs associations were used in this phase of OSINT. The main sources of data consisted of Institute of Health Information and Statistics (National Registry of Health Service Providers, 2026) and State Institute for Drug Control (2026).

Furthermore, healthcare software providers oriented on GPs (CGM World, 2026) were consulted to validate the choice of data streams and implications for the GPs obtained from these sources. Through the software provider consultations, contacts on GPs were obtained for further research. Since popular and widely known GPs (e.g. from the media) would not serve as representatives of the majority of the target group which generally remains known within its patient base rather than nation-wide, the research focused on regular GPs rather than public figures (GPs also active in state politics, influencers, writers etc.). Social media profiles were searched via obtained contacts using full names of the GPs. In line with the demography of the GPs with the majority over 50 years of age (Zítková, 27/05/2024), it is common to find their social media accounts using their full name and title.

The research focused on representation of solitary GPs as well as GPs operating within a healthcare facility (clinic etc.) or GPs cooperating with a university hospital. GPs from regions as well as GPs from larger cities were considered. The research showed that whereas solitary GPs run all aspects of the practice from care to investments in cybersecurity measures, GPs within a clinic are more likely to focus mainly on the primary care provided and let IT and security concerns be coordinated by the institution employing them. Furthermore, the research established that a lot of details concerning the state of IT and security of the given practice is disregarded in the process of practices being sold by senior GPs to their successors.

Overall, in this phase of the research, ten GPs were included representing all aspects of the target group stated above such as demography, location and type of practice in varying combinations. These GPs were subjected to all the phases of OSINT described in the paper. Expansion of the selected sample would possibly support or broaden the list of vectors described, however was not realised based on resource restrains of the research.

1.1.2 Background

OSINT seems to be the perfect method for today's data-driven society, the extensive amount of data available online making it almost impossible to approach and process information analysis without a sophisticated set of methods and technological tools that OSINT can use.

OSINT can generally be divided into technological OSINT (aimed mainly at the infrastructure, suitable for targeting larger institutions and IT suppliers) and "Spear"-OSINT (aimed at selecting and analysing individual users rather than broader infrastructure, suitable for targeting GPs). Several technological tools can, though, still potentially be used after the first phase of "Spear"-OSINT.

Among the technical ones, useful tools for OSINT worth mentioning comprise of OWASP ZAP, Nmap with Firewalk or Fierce used for locating non-contiguous IP space and hostnames that correlate with a specific domain. These methods can be used as a precursor to other tools such as Skipfish, Wapiti, Dirb or WPScan. At the same time, specific Google features are relevant for reviewing (DeCusatis et al., 2022). Oftentimes, it is recommended to check whether one's email address or phone number, but also electronic health record or other personal data has been leaked and used in cyber-attacks (Hunt, 2026), to which the leakage of credentials commonly contributes. For this reason, users are recommended not to use their job contacts for personal (i.e. e-shopping) purposes. At the same time, a person can create a separate email address for external inquiries.

GPs cannot influence the IP address or DNS much most of the times, therefore rather than focusing on technology, we focus on the users.

The common ground for OSINT and healthcare lies in the essence and importance of availability of information since both often use unverified sources (in one case, the Internet, and in another, the patient) to draw conclusions. Although medicine is known for its evidence-based practice, still until this day, doctors, and namely general practitioners (GPs), often rely on fragmentary statements of their patients, since medical documentation has up until now been largely carried out on paper that can be damaged or lost rather easily, or kept digitally without the complex connectivity needed to access it by any healthcare provider. Furthermore, both OSINT and GPs significantly value speed of information delivered. GPs are often the ones having to diagnose the symptoms first and, in most diseases, typical for this day and age, the stage in which they are diagnosed is crucial for the consequent care and probability of recovery.

Up until recently, sources for OSINT comprised of internet websites and news. However, today, social media generates a considerable amount of information on people's (nonexclusively general practitioners') opinions, whereabouts and lifestyles, therefore this source is also considered in the following OSINT.

1.2 The Human Factor

The healthcare sector relies heavily on the human factor. Since in healthcare, more often than not, technologies are outdated and lack of investments as well as staff is frequent, healthcare professionals learned to rely extensively on each other. That is why hacking tactics focusing on the human factor shall be especially effective in healthcare. This sector encourages solidarity and team spirit above all else which is why social engineering (as well as other human factor-oriented attacks) thrive in healthcare. Within the constraints of the sector, technical and physical cyber security measures do not sufficiently prevent social engineering and other attacks from succeeding (Patel, 2020) since the human factor (in this case, the user being the healthcare professional) is the main target that can be reached via other than technological methods described as follows.

One of the tactics for social engineering is fear or blackmail. For that reason, this paper investigates information accessible about the GPs that can be used as basis for not only fear or blackmail, but also other traits well represented among healthcare professionals such as empathy (Moudatsou et al., 2020), trust and authority (hand in hand with hierarchy). These can be triggered by attacker's tactics with emphasis on urgency, importance of the demand manipulating the healthcare professionals into human error (Adefabi et al., 2025).

The medical staff is expected to enhance its digital literacy as eHealth (Hummelholm, 2025) and wearable devices (Okpalanozie et al., 2025) spread across the patient care outside the hospital. Furthermore, despite persisting training efforts and the fact that training is generally outlined as among the most efficient measures, several healthcare professionals still feel insufficiently trained and informed on the topic of cybersecurity (Tikanmäki, 2025).

2. Results

2.1 Target Group Specification

The Czech Republic is the country designated for the OSINT due to it being located in Central Europe, between the former East and West European continent, nowadays a member of the European Union. The country comprises of approximately six thousand general practitioners and is divided into 16 administrative regions (National Registry of Health Service Providers, 2026). Several discussions about the uneven representation of healthcare professionals occur in the public sphere which is why the following figures demonstrate both the nominal representation of the GPs and their representation related to 100.000 inhabitants. Evidently, the differences among the regions when taking into consideration the number of inhabitants are not that severe.

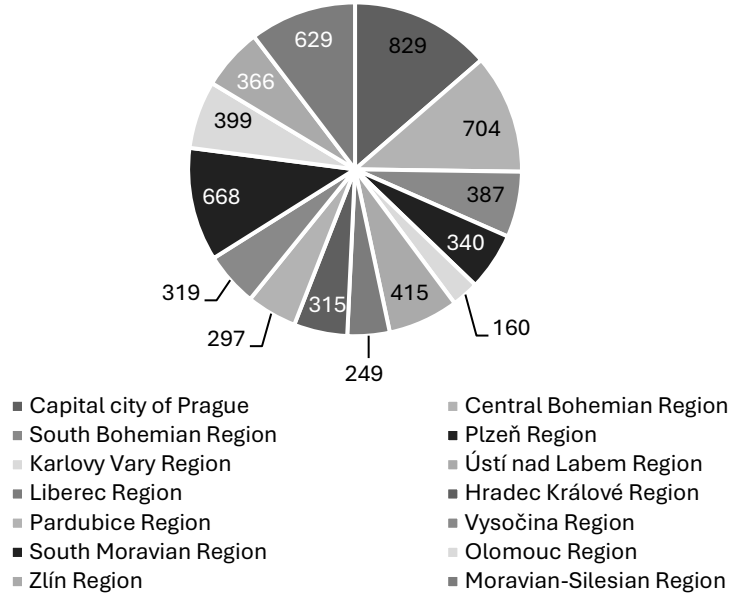

Figure 1: General practitioners density based on their belonging to a region

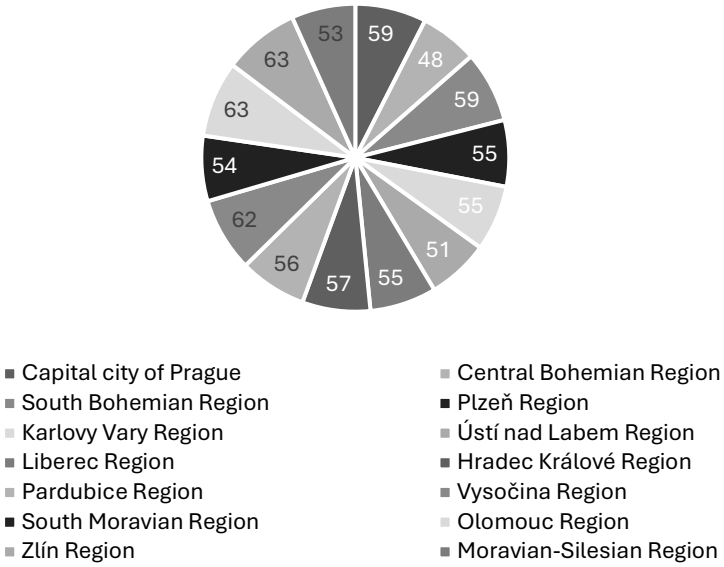

Figure 2: General practitioners density based on their belonging to a region after correction of GP per 100.000 inhabitants

The OSINT is demonstrated on a set of GP representatives (Institute of Health Information and Statistics, 2026) who were selected according to their affiliation to a region and their practice's organisational structure (such as a simple private practice, belonging to a clinic or cooperation within a university hospital) to ensure diversity. Other aspects could be taken into account during the selection, such as the number of registered patients or amount of care provided, however this information is not publicly available. The demographic data presented in the figures serves as basis for identifying the key representatives of the target group of GPs for further OSINT and subsequent research comprising of structured interviews and indicates bias in media and political communication emphasising underrepresentation of GPs in regions outside of large urban areas.

The data used for the research is accessible in national registries in real time since each GP has a legislative obligation to notify the Czech Medical Chamber (2026) in case of any changes which are then reflected in the datasets.

2.2 Social Media

Social media (mainly Facebook and Instagram) was used as some of the key sources of information for the OSINT since it is proven to influence public opinions upon inviting emotional and therefore rapid reactions (derived from dopamine or anger, without further consideration of consequences that the user's reaction might have in the long-term perspective) by promoting the most engaging content (Damons, 2025). This way, a lot of formerly deterministic issues are now becoming political with contesting the argument of factual truth (promoting misinformation and propaganda potentially leading to undermining trust in institutions) which is a trend encouraged by most political powers now also present on the social media.

In the context of GPs, social media accounts customarily being registered via email address of the user, the GPs frequently do not distinguish private from public life which is why they may often use the same email address for social media as well as contact with patients. However, emails have been repeatedly the vector of attack of social media accounts since the users, seeing the amount of attacks and fraud on social media, strengthen their social media account password, but forget to strengthen their backup email password through which the attacker may even change the rather secure social media password, pretending to be the original user who forgot the initial secure credentials. A vector specific to GPs is at hand: since the attacker accesses the email, they can not only enter social media accounts, but also contact patients via email distributing misleading information, phishing etc. At the same time, conversations carried out within social media platforms can hardly be considered private (Damons, 2025). Not all communication on these platforms is carried out among "real" human beings (e.g. bots and fake identity profiles are used extensively).

One of the main weaknesses of the current level of Czech healthcare largely relies on elderly medical professionals (Zítková, 27/05/2024). Although it is apparent that social media is most common among younger generations, the elderly often make an effort to enter this space for the sake of connecting with their grandchildren (mostly for family pictures and calls) and not being so keen in the virtual space makes them exceptionally vulnerable. This is most prevalent in the digital footprint of the GPs who often reflect publicly on emotion-triggering political or socioeconomic issues, showing their true colours without realising that these can be used against them by any patient or alien. The recommendation to change one's username even slightly as opposed to real full name already makes one considerably less searchable (and therefore more secure) on social media.

Healthcare is especially susceptible to social engineering because of the generally high trust factor. Data breaches have been reported based on posting images of hospital employees with sensitive data such as passwords shown unintentionally in the background (Patel, 2020).

Another source of sensitive information is reviews on Google or GPs' websites. The reviewers on these platforms (presumably mostly patients) do not hesitate to mention personal comments on behalf of the GPs such as specify location of both the practice and their home (especially in case of small-town patient base), family members of the GP (in one case, the patient mentions that it is admirable that the GP answers phone calls from patients even though she has two small children etc.). Not only the identity of the GP, but also the one of the patient/commentator can get revealed. The specific information revealed can later be used by an attacker impersonating either the patient or the GP while attempting to compromise one or the other.

3. Discussion and Conclusion

3.1 Use of Artificial Intelligence in OSINT

Different LLMs can be used to broaden the amount of information investigating a specific GP. A current affair with X's Grok creating revealing images with body details only based on private conversations (CCDH, 2026) seems to open doors to larger datasets than a regular user would dare (and possibly fear) to imagine, whereas other common LLMs still impose barriers on private matters on the GPs. For example, although a review mentioned the number of children of a GP, ChatGPT -5.2 (in free version) (OpenAI, 2026) did not disclose this information even upon specifically asking for it. The future of AI remains vague although authorities have been trying to tackle its security and safety issues ever since the LLMs became widely accessible to the general public (EU, 2026). Though industry generally develops faster than regulations, and specifically AI and IT industry develop in the fastest pace, therefore their security and privacy issues remain a great question mark.

While the healthcare system, governments and legislation are debating how to incorporate AI into healthcare and together with the digitalization utilize it in favour of care accessibility despite the demography (in form of increase of aging population and decrease of medical staff), LLMs are with or without needed certifications used in healthcare nowadays. The staff does not hesitate to use these models with or without instructions from the cybersecurity department to minimise their efforts on the tasks not directly linked to providing care to the patient (e.g. documentation). For these tasks, the staff often consults publicly accessible LLMs, sharing details of the patient as well as their practice. These details can, in cooperation with the LLMs, be used for OSINT later on. At the same time, LLMs do not only help decrease the workload of the staff but might bring more patients to the facility given that cases where LLMs suggested medical advice that caused harm to the patient are documented (Antivirus, 2026). With today's inevitable rise of AI, it is apparent that just as social media, AI is increasingly becoming a source of information for (not exclusively) OSINT. With its expanding database of information on GPs and their patients, AI (if not well-regulated) can also provide valuable insights to attackers.

3.2 Conclusion

When entering cyber space, GPs should take into consideration the global picture they paint in society which is often the picture of authority that others look up to. When posting content, reacting and showing affection towards a certain political group or ideals, it is recommended for the GPs to approach this the same way other public figures do, e.g. create separate (slightly anonymous) accounts for leisure and others (with full name and real profile picture) for public presentation. Social media users frequently forget is that their digital footprint is always trackable and anything can later be used against them. Switching among multiple accounts is a standard feature for most social networks so it does not considerably decrease the user experience.

All OSINT outcomes together with cybersecurity recommendations drawn from them should always be verified in the real-world settings which is why the research is planned to continue via structured interviews with the GPs. Therefore, the impact of the OSINT outcomes may be measured in the context of the specific GPs. For the sake of keeping the selected GPs anonymized, specific sources of reviews and social media accounts that would identify them have been left out.

When it comes to specific OSINT findings and their connection to exploitation, while younger GPs might accidently reveal their credentials taking pictures on social media with background containing passwords to clinical software, older (quite more represented) generation of GPs might be more susceptible to giving their credentials to a stranger on the phone claiming that they are the software provider or a government/public representative. Both examples reflect potential harm to the healthcare professionals as well as their patients.

Ethics declaration: No ethics declaration was needed for this research.

AI declaration: AI was used in the dataset gathering phase as one of multiple information sources.

References

Adefabi, R., Onimole, O., Sani, A. I., Olajide, O., & Okpalanozie, V. (2025). Cognitive Hacking and Social Engineering in Healthcare: Exploiting Human Behaviour. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 1-8. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

Antivirus. (2026). *Antivirus: Google's AI gives people incorrect, sometimes dangerous health advice, warns The Guardian*. Czech Radio. Retrieved February 22, 2026, from https://radiozurnal.rozhlas.cz/antivirus-ai-od-googlu-radi-lidem-o-zdravi-chybne-nekdy-i-nebezpecne-varuje-9588436

Bracciale, L., Loreti, P., & Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-45927-1

CCDH. (2026, January 22). *Grok floods X with sexualized images of women and children*. Center for Countering Digital Hate. Retrieved January 25, 2026, from https://counterhate.com/research/grok-floods-x-with-sexualized-images/

CGM World. (2026). Retrieved February 22, 2026, from https://www.cgmsvet.cz/

Czech Medical Chamber. (2026). Retrieved February 22, 2026, from https://www.lkcr.cz/

Damons, D. (2025). Weaponizing Connectivity: The Role of Social Media and Cyberspace in Modern Subversion. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 857-863. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

DeCusatis, C., Peko, P., Irving, J., Teache, M., Laibach, C., & Hodge, J. (2022). A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Systems. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 0760-0764. https://doi.org/10.1109/ccwc54503.2022.9720785

EU. (2026). *AI Act*. EU Artificial Intelligence Act. Retrieved January 25, 2026, from https://artificialintelligenceact.eu/the-act/

Hummelholm, A. (2025). E-Health Systems for Remote and Disaster-Resilient Digital Environments. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 204-213. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

Hunt, T. (2026). *Have I Been Pwned*. Have I Been Pwned. Retrieved January 25, 2026, from https://haveibeenpwned.com/

Institute of Health Information and Statistics. (2026). *Healthcare in the Czech Republic: Staff Capacities and Remuneration 2024*. Institute of Health Information and Statistics. Retrieved January 25, 2026, from https://www.uzis.cz/index.php?pg=aktuality&aid=8729

Moudatsou, M., Stavropoulou, A., Philalithis, A., & Koukouli, S. (2020). The Role of Empathy in Health and Social Care Professionals. *Healthcare*, *8*(1), 26. https://doi.org/10.3390/healthcare8010026

National Registry of Health Service Providers. (2026). *Map of Providers.* National Registry of Health Service Providers. Retrieved January 25, 2026, from https://nrpzs.uzis.cz/index.php?kraj=CZ080&okres=&obec=&obor=L44&forma=ćrum=&Submit=Vyhledat&pg=mapa-poskytovatelu&ids=&token=44486f14e0615e6c8c7200e989ac0ccdca2943ab01f578d176f8d33f66e7ea65

Okpalanozie, V., Adeleye, O., Adefabi, R., Onimole, O., & Osamor, J. (2025). Cyberbiosecurity in Healthcare: Securing Medical Devices from Digital and Biological Threats. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 481-489. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

OpenAI. (2026). *ChatGPT*. OpenAI. Retrieved January 25, 2026, from https://chatgpt.com/

Patel, N. (2020). SOCIAL ENGINEERING AS AN EVOLUTIONARY THREAT TO INFORMATION SECURITY IN HEALTHCARE ORGANIZATIONS. *Jurnal Administrasi Kesehatan Indonesia*, *8*(1), 56. https://doi.org/10.20473/jaki.v8i1.2020.56-64

State Institute for Drug Control. (2026). Retrieved February 22, 2026, from https://sukl.gov.cz/

Tampu, F., & Berek, L. (2025). Potential Use of Open-Source Intelligence (OSINT) in the Public Health and Epidemiology Sector of Medicine. *Orvosi Hetilap*, *166*(32), 1250-1255. https://doi.org/10.1556/650.2025.33370

Tikanmäki, I. (2025). Cybersecurity Training in the Healthcare Domain. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 674-681. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

Tikanmäki, I., Blek, T., Niskakangas, J., & Varamäki, K. (2025). Enhancing Cybersecurity in Healthcare: The KyberSoTe Project's Approach to Mitigating Cyber Threats. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, *24*(1), 665-673. https://papers.academic-conferences.org/index.php/eccws/issue/view/48/66

Zítková, P. (27/05/2024). *Who will treat us in 10 years? Pediatricians, general practitioners, surgeons, diabetologists and pathologists will soon be an endangered species*. Our Healthcare. Retrieved January 25, 2026, from https://nasezdravotnictvi.cz/aktualita/kdo-nas-bude-lecit-za-10-let-pediatri-prakticti-lekari-chirurgove-diabetologove-i-patologove-budou-uz-brzy-ohrozenym-druhem