ISSN: 2956-0179
eISSN: 2956-0306

ANNALS OF NURSING

A QUARTERLY INTERNATIONAL JOURNAL

THE OFFICIAL
JOURNAL OF THE
MEDIKA COLLEGE
FOR VOCATIONAL
STUDIES IN
HEALTHCARE
BELGRADE
SERBIA

VOLUME 1, ISSUE 2, 2023

Annals
of Nursing

ISSN 2956-0179

e ISSN 2956-0306

Annals of Nursing

A Quarterly International Journal

The Official Journal of the Medika College for Vocational Studies in Healthcare

Belgrade Serbia

Volume 1, Issue 2, January-March 2023

Annals of Nursing

A Quarterly International Journal

Editor-in-Chief

Goran Belojević

Publisher

Medika College for Vocational Studies in Healthcare

Belgrade

Printing Company

School Service Gajić

Belgrade

Print run

250

ABOUT THE JOURNAL

„Annals of Nursing" is the official journal of the Medika College for Vocational Studies in Healthcare, Belgrade Serbia. It is a quarterly international open access peer-reviewed journal that covers all aspects of nursing in hospitals, families, and the communities. The papers published in "Annals of Nursing" are freely available to all internet users for non-commercial use. The focus of the journal is on the role of nurses in the promotion of health and the quality of life, prevention of illness, care of disabled and ill people and all suffering individuals and rehabilitation after illness.

EDITORIAL BOARD

TABLE OF CONTENTS

Annals of Nursing, Vol 1, Issue 2, January-March 2023

Review Article

CYBERATTACKS ON HEALTHCARE SYSTEMS

Jasmina M. Veličković, Katarina Jonev Ćiraković

Medika College for Vocational Studies in Healthcare, Belgrade, Serbia

Received: 6 February 2023**; Revised:** 27 February 2023**; Accepted:** 4 March 2023;
Published: 17 March 2023

DOI: 10.58424/annnurs.tx5.mdn.v5p

Abstract

Cyberattacks on healthcare information systems have become more frequent in the last few years. The consequences are not only the collapse of a system and a financial damage, but also a direct threat to the patients' health and lives. The basic methods and techniques of stealing health data from end users of the internet and the use of stolen data to commit criminal acts are presented in this paper. Numerous cyberattacks on healthcare systems worldwide are reviewed and analyzed, with a focus on the COVID19 pandemic. In recent years, the international community has intensified its work on legal regulations and conventions and raising awareness concerning the cyber security of healthcare systems. Cyberattacks on healthcare systems are a global problem, and the solutions should be global, as well.

Keywords: healthcare, internet, information system, crime

Corresponding Author: Jasmina Veličković, jasminav.frad@gmail.com

Introduction

The rapid development of information and communication technologies (ICT) and their application have become an inevitable factor in shaping social life, which provides the possibility of new ways of communication, information, education, work, and entertainment. Due to the emergence of new technologies and digital performances that make it possible to simplify the life of users, healthcare is increasingly evolving towards digitalization. On one hand, this represents a great opportunity, but it also exposes healthcare organizations to multiple threats in connection with the security of the process and potentially the security of patients themselves.

By supporting financial and administrative transactions, public health surveillance, professional education, and biomedical research, the Internet has lowered the administrative costs of healthcare, improved public health, obtained better-trained healthcare providers, and led to new insights into the nature of disease[1]. At the same time, ICT tools are efficient mechanisms for collecting important information for public health. The example is online reporting of medical laboratories on test results for some infectious diseases, such as COVID-19 or tuberculosis. The automated systems reduce the cost of public health data collection[2] .

However, with all the advantages of digitization of healthcare, unfortunately there are also many abuses. The public health system depends on public trust that sensitive health data is used only for the benefit of patients. Such data must be protected both during transit (sending) and while being stored on computers in the offices of health institutions. Cyberattacks lead to jeopardizing the functioning of the systems of health institutions that base their work on ICT tools, and Internet criminals often corrupt data to gain blackmail and financial power.

Although many monographs and works were published about computer crime in the past decades, no significant progress was made in terms of a comprehensive definition[3]. The first definition of computer crime comes from 1979 and is given in the Computer crime: criminal justice resource manual and states that computer crime is "any illegal act for the successful prosecution of which a good knowledge of computer technology is necessary"[4]. Cybercrime is a very complex form of crime that has great dynamism, constantly expands, and develops new forms, has no territorial limitations, and practically with no state borders or geographical limitations[5]. The global network has great advantages for the application and spread of crime, it provides the possibility of easy association of criminal groups from different areas of the world and is a good hideout for them.

Cyberattacks on healthcare infrastructure are on the rise and the potentially catastrophic consequences must not be ignored. Therefore, healthcare workers are tasked with the constant implementation of new knowledge in the field of Internet use, as well as the ability to protect and respond to incidents that may occur. Due to the lack of organized statistical bases and a generally accepted methodology for recording cybercrimes on a global level, it is very difficult to obtain precise parameters about the scale, size, and scope of global cybercrime in the sector of healthcare. By searching the available literature and legal documents in the field of cybercrime, one gets the impression that cybercrime unstoppably penetrates and destroys all spheres of society, despite all the efforts made at the domestic and international levels to ensure the protection of Internet users. As the knowledge and skills of cybercriminals increase, so does the need for more effective prevention and detection of these criminal activities.

With the occurrence of cyberattacks in the 1970s, cyber security has become an essential segment of almost every organization. Research on cyber security has grown significantly in the last two decades[2], indicating an increasing concern about attackers who could threaten the work of organizations, systems, and institutions[6]. From storing patient information in the cloud to using artificial intelligence for radiology screening, medicine's increasing reliance on technology introduces new risks.

Computer attacks threaten not only the functioning of the system, but the health and lives of people as well. With the development of the Internet and cyberspace itself, cybercrimes of various forms have evolved. Although there is no global consensus on what constitutes illegal activities on the Internet, most academics and security experts agree that cybercrime is one of the fastest growing forms of crime[7].

This study aimed to identify the major topics and concerns in today's healthcare system and hospital cybersecurity.

Types of cyberattacks on healthcare systems

Phishing is a cyberattack manifested in sending a mass message, usually via email. Social engineering is exploited to influence at least one of the recipients to open the message, and either navigate to a website or download a file that has been rigged with malware. Deception of the recipients often involves the message appearing to originate from reliable sources, such as peers or information technology (IT) employees. In general, phishing is the most common delivery method for offenders to infiltrate healthcare systems, with 89% of cybercrimes being initiated via phishing emails[8].

Denial-of-Services (DoS) accounts for 48% of cyberattacks. DoS involves actors "flooding a network with traffic" to the point that the network is overwhelmed to respond and thus cannot be accessed. Usually intended to ruin the hospital's reputation or physically harm patients , a DoS event can prevent medical teams from retrieving or sending patient data and can be expensive for the hospital to recover the network[9] .

A subtype, *Distributed Denial-of-Services* (DDoS) refers to DoS incidents that utilize several computers or other machines, usually internet bots, to perform the attack. More source computers enable a more formidable and incognito attack[9]. More recently, the US Department of Health and Human Services website experienced an attempted DDoS attack, just as people increasingly wanted to access the site during March 2020's COVID-19 outbreak.

Administrative access can enable attackers to infect systems with more severe malware than regular accounts could achieve. A data management software, Philips IntelliSpace Perinatal, was found in 2019 to be vulnerable to privilege escalation attacks, which could be carried out by amateurs. Often in healthcare, Man-in-the-middle (MITM) incidents lead to the leaking of sensitive patient information or manipulation of medical data, which can then be sold, repurposed to commit other cybercrimes, or even used to intimidate or extort affected patients[10].

Cryptographic attacks, which enable hackers to surveil, steal, modify, delete, or otherwise damage patient records or other confidential information, can involve encrypting a hospital's data, decrypting it, or decrypting and then re-encrypting with another key. Oftentimes, hackers encrypt data to block access to its content until a ransom is paid, commonly known as a ransomware attack. For example, ransomware targeted hospital computers and devices around the world in the 2017 WannaCry attack (described in “Consequences” section), an event regarded in healthcare as “one of the most impactful cyberattacks in history”.

Spoofing is a method in which hackers attempt to influence a medical device to receive an external signal, thereby allowing them to access or adjust the data, operations settings, and other system components[11].

The utilization of drones is a new attack method gaining momentum. Drones, also called unmanned aerial vehicles (UAVs), offer hackers the ability to be close enough to access almost any facility's network (current methods recommend that attacks be carried out within 10 meters). A small UAV was shown in two experiments to be able to be situated over hospitals, even ones in difficult-to-reach locations, and hack the networks without being noticed[11].

Historical data about cyberattacks on healthcare systems

In 1989, a scientist at a World Health Organization AIDS conference knowingly distributed 20000 floppy disks containing a malicious virus called AIDS. After the diskette was inserted into the computer, the virus took control and locked the documents. As the perpetrator promised a decryption key in exchange for money, this incident not only became known as the first documented ransomware attack, but also one of the first cyberattacks on the healthcare system[12]. Since then, threats in the healthcare sector have evolved.

Cyberattacks are growing exponentially[13] and by 2019, 24% of them were in the healthcare industry[14]. During 2014–2016, 90% and 45% of hospitals and clinics experienced at least one and five data breaches, respectively[15]. In a British hospital during one-month period 2.2% of emails and 2.9% of website actions were reported as suspicious[8]. In 2018, a phishing incident at Baylor Medical in Texas exposed the personal information of 47,000 patients[16]. In the same year, the medical information of the country's prime minister and 1.5 million other patients was stolen in Singapore.

Since 2015, hacker attacks have been one of the main reasons for leaking medical records. This coincided with the moment when American institutions digitized health records, and switched to tools such as monitors that are connected to the Internet[12]. The electronic health record is a digital version of the patient's medical record. Each electronic health record contains information on patient demographics, insurance information, mailing address, social security number, date of birth, prescribing physician's notes, lifestyle details, list of prescribed medications, family medical history, vaccination records, lab results, and even radiology reports among other things. In addition to medical records, records may also contain billing information such as credit card information and payment of expenses. The most common type of attack associated with cybercrime is in the form of a data breach. The electronic health record is a digital version of the patient's medical record. Each electronic health record contains information on patient demographics, insurance information, mailing address, social security number, date of birth, prescribing physician's notes, lifestyle details, list of prescribed medications, family medical history, vaccination records, lab results, and even radiology reports among other things. In addition to medical records, records may also contain billing information such as credit card information and payment of expenses[12].

The greatest impact of health record theft is noticeable in countries where most citizens have health insurance. In 2016, 91% of the US population had health insurance. Therefore, any major system security breach in the US healthcare organization could affect many citizens[12]. Data theft, apart from directly affecting the victim, his privacy and identity, can also lead to the complication of the criminal act. Namely, many of situations have been recorded in which, after the theft of personal data, cybercriminals used it to buy drugs, for tax fraud, identity theft and similar actions. Victims of data breaches are often not aware that their personal data has been stolen, nor that the stolen data is being used in a criminal act[17].

In May 2017, self-expanding WannaCry ransomware hit systems in 150 countries, including digitized healthcare systems[12,17]. For example, in Great Britain, due to the attack on the health system, the work of health institutions, especially hospitals, was disrupted, which led to over 19,000 canceled appointments for patient examinations and operations. The WannaCry ransomware was used to encrypt and lock computers, and the attackers demanded a ransom payment in bitcoins to decrypt them. The virus exploited a vulnerability in the Windows operating system. Problems with medical devices, such as MRI scanners, have also been reported[12,17].

In September 2020, the Vastamo psychotherapy center was the target of blackmail and threats regarding data stolen in November 2018 and March 2019[12]. Vastamo has 25 therapy centers throughout Finland. Data on about 36,000 patients, including minors, were stolen. This data contained highly sensitive personal health information, including information about the therapy sessions of the vulnerable[17].

Cyberattacks during the COVID19 pandemic

Recent research suggests that the COVID19 pandemic-related cybercrime involves patients' and healthcare institutions' data theft, disruption in the distribution of protective equipment, pharmaceutical and sanitary products, false COVID tests and COVID vaccines, various forms of scam, different covid-themed campaigns with hidden agendas and numerous disinformation campaigns with compromised email addresses of state institutions, companies and individuals, social engineering, etc[18].

The COVID-19 pandemic brought to the forefront further gaps in hospitals' cyber preparedness, demonstrating the insufficiency of current protective measures. Cyberattacks rose during 2020, particularly ones involving ransoms: hackers targeted a Czech hospital, UK vaccine trial, US health agency, UK emergency COVID-19 hospital construction team, and US, UK, and Canadian vaccine development labs, just to name a few. The attacks became so prevalent that governments and the international policing agency INTERPOL released alerts regarding the threats. In the US, cybercriminals compiled a list of more than 400 vulnerable hospitals to target and attacked quite a few[19].

The COVID19 pandemic caused concern due to a convergence of hostile activities in the virtual space. Healthcare is increasingly under attack because of the combination of three factors:

● Healthcare services are crucial as patients' well-being depends on it. This made hospitals a target for digital extortion and attacks.

● Healthcare is a repository of valuable and sensitive data such as medical documentation and vaccine research which makes it an attractive target for data theft and cyber espionage.

● Healthcare found itself in the center of a strategic international rivalry over the pandemic growing into malicious activities such as disinformation campaigns against the sector[18].

An example of a big attack during the pandemic and an illustration of the previously explained complication is the attack on the national healthcare agency of the USA. It was a DDoS attack that not much is known about because the USA has hidden most the information from experts and the public and this problem is handled by the national agencies of the USA[10]. The second big attack happened in the Czech Republic, and it was directed against one of the largest hospitals that carried out testing in the initial stages of rapid COVID spread across Europe. This one, as well, was a DDoS attack whereby it can be inferred that health institutions indeed are the new main targets, although they have already been assailed by malware and other sorts of cyber abuse. Hackers attacked and crashed the IT systems of the company that schedules vaccination against COVID19 in the region of Lazio, near Rome[20].

Some of the recorded and publicly available data on cyberattacks during the pandemic is:

-University Hospital Brno (the Czech Republic) - IT network deactivation causing urgent surgeries delay and jeopardizing the operation of the emergency ward[12].

World Health Organization - the development of a malicious website emulating the internal email system with a view to steal employee passwords[17].

- In the UK, a lab researching a COVID19 vaccine - ransomware attack resulting in the distribution of ex patients' personal information and a failed attempt to disable the network[21].

- Hospitals in Paris – a series of attacks against hospital servers[22].

- The healthcare systems in Spain - a ransomware attack aiming to deactivate the software with patient data[23].

In 2021. 45 million individuals were affected by attacks on healthcare compared to 34 million in 2020. That number tripled in only three years - from 14 million in 2018[24].

Aside from healthcare services, the medical equipment industrial supply chain is also susceptible to cyberattacks. Intellectual property theft from research institutions working on new treatment methods, diagnostics and vaccines was a special problem. At the beginning of May 2020, the National Cyber Security Center in the UK declared a substantial increase in the number of cyberattacks committed by hostile states and cyber criminals against British universities and institutions researching COVID19[25].

Consequences of cyberattacks on healthcare systems

Twenty percent of cyberattacks cause financial injury. Moreover, healthcare is the industry that spends the most money on dealing with data breaches, a whopping $7.13 million on average worldwide. In comparison, the average cost of data breaches in all industries worldwide is $3.86 million[26].

While financial loss incurred by a hospital due to cyberattacks is one of the most publicized consequences, one of the most damaging is the negative effects on the hospital's reputation. A data breach can inculcate a sense of distrust between patients and healthcare providers[26]. Decreased trust will, in turn, make patients less likely to share personal information with providers, including information that may be clinically significant[26]. The fact that an estimated 67% of hospitals do not have programs in place to assist patients whose data has been exposed can further damage trust relationships following an attack.

A troubling potential consequence is a physical harm to the patients[26]. Fifty-five percent of attacks in recent years interfered with hospitals' networks and services, and 18% interfered with or damaged systems necessary for medical care. Incidents have caused critical patient injury[26]. At the ancillary level, digital hospital equipment, like computer-run elevators needed to transport patients or lab samples and computer-run Heating Ventilation and Air Conditioning

(HVAC). HVAC systems needed to maintain sterility in operating rooms, can be shut down or made to malfunction.

Medical devices can be categorized according to their purposes: diagnostic, monitoring, and therapeutic[27]. Diagnostic devices are used to identify a patient's medical state, such as determining the cause of a patient's symptoms. This category includes ultrasounds, EKGs, pathogen identification test systems, and more. The most common category, monitoring devices, provide continuous observation of a patient's health, alerting when physiological indicators deviate from baseline values[26].

There are several potential sources of cyber risks in telehealth. First, the patients, especially in older populations, do not usually know how to protect from cybersecurity threats on their end. When using the telehealth system, they may have easily guessed passwords, accidentally expose their device or the telehealth software, fall victim to phishing attacks, or end up misplacing the device connected to the telehealth system (and by extension the sensitive information.

Cyberattacks harm victims in the following ways: they can suffer the consequences of leaking personal information (for example of a financial nature) and become victims of medical identity theft which has serious consequences for health insurance in the USA.

A question was thus advanced: are hospitals prepared for the risks that accompany clinical medicine in cyberspace? This study aimed to identify the current trends in healthcare cybersecurity according to a basic 4-point outline: (a) the major clinical uses of cyber technology and their security risks, (b) secondary risks associated with the technology, and (c) current strategies healthcare institutions have in place to combat the threats. Risks and strategies were compared to elucidate the security gaps. Analysis was concluded inductively, with patterns, of cybersecurity strengths and failures examined separately, then considered under the scope of real-world incidents. There are several types of actors involved in the cyberattack industry, including criminals, “hacktivists,” terrorists, spies, and ethical hackers, differing primarily by their goals, levels of credentials, and lawfulness. If these characteristics, especially the motives, of potential attackers are known, hospitals can better institute cybersecurity measures[28]. Four primary motives were identified in the literature.

The most common motive of attackers is money[30], accounting for 91% of data breaches [31]. Each patient record is worth an average of $50 on the darknet, and a complete set of medical records can earn up to $1,000. A social security number, in contrast, is valued at a mere $1. Additionally, ransomed data is worth a lot, as it can also be sold to another criminal who will use it to extort the hospital again[29].

Stolen data can be used by hackers or their darknet customers to fraudulently apply for loans or other financial programs or receive identification (ID) documents[30]. Patient ID data can, for example, be used to request free medical insurance coverage, like Medicare . Medical provider ID credentials, especially, can expand a hacker's access to the hospital network[29] or enable falsification of medication orders to sell the drugs on the darknet[30]. As such, while other industry credentials are worth dimes[29], medical credentials are worth much more.

Attackers may act on behalf of a political goal. During an international war, an attacking country may attempt to prevent the target nation from providing medical treatment to its citizens, harm the citizens by altering medical device operations, or uncover confidential information that can be used against the target country. Four percent of attacks are due to espionage[21]. The offending group may also choose to attack for propaganda purposes. In 2017, the terror group ISIS hacked into the UK's National Health Service (NHS) website and posted images from the Syrian civil war, as part of its propaganda efforts[23].

Criminals may act to disrupt healthcare services for the very purpose of disrupting services. Causing DoS, introducing ransomware, or infecting medical devices, for example, may be the end goal.

Cyberattacks committed by state actors and across borders are some of the most formidable. It is challenging to pinpoint and eliminate the attackers, and events often go unnoticed.

Among other justifications, these attacks may be carried out for personal enjoyment, as are 5% of attacks, or may be in retaliation for a perceived slight on the part of the hospital or a physician, as are 1% of attacks[32].

- Primary infiltration refers to an attack that directly impacts, maliciously or not, a hospitals' patients.
- Secondary infiltration occurs when the attack impacts the patients by implication only, not directly. Primary-level incidents may be strengthened by secondary-level activities.

Once inside, the attacker assesses the system for what information or capabilities it has, specifically repositories of user account information, electronic medical records, medical device connections, and financial information, such as billing data. The assessment then turns to the databases chosen for infiltration, gauging their usual traffic and vulnerabilities. This is a critical step that will help the party enter, operate, and exit, while evading detection. The climax is then reached when the attacker targets the vulnerabilities and steals information from, shuts down, modifies, or impedes the network[33].

Protection against cyberattacks on healthcare systems

The current information age has put the protection of data, information, and cyber security in the foreground, as an important aspect of individual, organizational, state and international security. According to the ISO/IEC standard, cyber security means "preserving the confidentiality, integrity and availability of information" among other characteristics[34].Many healthcare institutions do not invest in cyber security, despite the attacks increment. The largest attack in 2021 hit a hospital in Florida (Florida Healthy Kids Corporation), when about 3.5 million users were affected. One of the main trends established through comparison of all available, recent, and relevant literature is that serious gaps are present in hospitals' approaches to technical, educational, policy, and resource-allocation elements of cybersecurity. Cybercriminals can access, steal, block, or manipulate screening tools, medication treatments, vital sign alarms, patient records, telecommunication, or clinical supplies, just to name a few. Yet, hospitals lack adequate protection for each of these vulnerabilities.

The first step in attack prevention is being aware of the risks[34], as this paper aimed to do. As shown in this paper, however, many of these findings are still areas of concern in the field. Perhaps the most crucial takeaway is that when cyberattacks occur in hospitals, patients are the real victims[35]. Most confidential data that hackers compromise belongs to patients, and it is their health on the line when medical devices are manipulated, hospital computers are rendered inoperable, or treatments are inaccessible. If not for financial, reputational, or functional reasons, then at least for the sake of their patients, hospitals should actively work to prepare themselves for the inevitable cybersecurity risks.

Current cyber protection actions undertaken by hospitals most often relate to security on the user's end, be it the medical provider's and/or the patient's end. Some actions involve allowing navigation only to specific websites, requiring difficult-to-guess and regularly changed passwords, and allowing connections to the hospital network only by facility-approved devices[31]. These specifications are intended to make computers, accounts, and networks less vulnerable, but they are often not enough to prevent breaches. For example, the thirty most attacked vulnerabilities in 2015 were password-independent[36].

Network vulnerabilities may also be attributed to weak hospital cybersecurity departments. Seventy-three percent of healthcare organizations are incapable of managing cyber incidents[13]. Most IT departments do not run complete risk evaluations of the networks , with only 16% scheduling evaluations of system vulnerabilities more than annually. Twenty-nine percent reported not having cyberattack response plans whatsoever[15], and of those who do, 80% have not actually tested their cyber incident protocols[7].

On the IT department's end, active steps taken include segmentation and patching[36]. Segmentation refers to separating the hospital network, including the devices connected to them, into small sections. Even if a malicious actor succeeds in infiltrating one of these sections, the others remain secure. Like using cloth patches to cover holes in clothing, patching is a method of covering software vulnerability “holes.” When a vulnerability is found in a system's code, the manufacturer will usually release a patch, sometimes in the form of a program upgrade[10]. IT departments themselves are also often on the lookout for vulnerabilities in their systems.

Health information is one of the most confidential datasets that exist. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 recognized this and mandated protections for sensitive health information. Therefore, demographic data, medical and mental history, test results, insurance details, and information providers need to care for patients are protected under the law[37]. One requirement of HIPAA is that data breaches of more than 500 patient records must be reported and patients informed[36]. So large a breach was unlikely, until edical databases came into being. At that point, further security standards were necessary to manage the novel risks cyber technologies were creating.

Many hospitals rely on government regulations and guidelines to inform their cybersecurity practices. For instance, per HIPAA regulations, each hospital must designate a data security officer, regularly perform risk assessments, and have incident response plans prepared. Nevertheless, regulations can be too basic to effectively protect hospitals, like the Centers for Medicare and Medicaid Services mandating only simple antivirus and antimalware tools for hospitals using their services[36].

Conclusion

The multiplication of attacks on healthcare systems, especially during the COVID19 pandemic posed a global threat to human health and lives. Considering the insufficient examination of the cyberattack phenomenon the documented effects of convergent threats cause concern: disruption in patient care, loss of faith in the cyber security sector in general, and concern for patient data, while disinformation campaigns induce fear and doubt towards the sector causing confusion and detriment to the whole society. Future studies from healthcare cybersecurity industries are expected to improve the cyber protection of healthcare systems.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Lupton D. Medicine as culture: illness, disease, and the body. Newcastle: Sage; 2012.
2. Faria NMS, Campilho RDSG, Silva FJG. Concept and Design of Automated Moving Device for Healthcare Equipment. FME Transactions 2021; 49: 598-607.
3. Leiner BM, Cerf VG, Clark DD, et al. Brief history of the Internet. ACM SIGCOMM Computer Communication Review 2009; 39 (5): 22-31.
4. Computer crime: criminal justice resource manual.1979. Delhi, India: Gyan Books Pvt. Ltd.; 2022.
5. Đukić A. Krađa identiteta - oblici, karakteristike i rasprostranjenost. Vojno delo 2017; 69 (3): 99-118.
6. Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. J Med Int Res 2019; 21:e12644.
7. Radulović S. Pretnje visokotehnološkog kriminala i domaća zakonodavna regulativa. Revija za bezbednost – stručni časopis o korupciji i organizovanom kriminalu 2008; (2) 8:18.
8. Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: threats, mitigation and approaches. BMJ Health Care Inform 2019; 26(1):e100031.
9. Houlding D. How do your cybersecurity efforts stack up? Being prepared will make you less likely to become a soft target. Health Manag Technol 2017; 38: 26–7.
10. Cybersecurity and Infrastructure Security Agency. ICS Medical Advisory (ICSMA-19-297-01) Philips IntelliSpace Perinatal; 2019.

11. Sethuraman SC, Vijayakumar C, Walczak S. Cyber attacks on healthcare devices using unmanned aerial vehicles. J Med Syst 2020; 44:29.

12. Matijasevic J, Spalevic Ž. Specific characteristics of computer criminal offenses with regard to the law regulations, XLV International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2010 CONFERENCE, 23–26. June 2010, Faculty of Technical Sciences, University „St. Clement Ohridski“, Bitola, Ohrid, Macedonia; 2010.

13. Becker's Healthcare. Cyberattacks on Healthcare Providers Expected to Triple Next Year: Black Book Report 2020.

14. Martignani C. Cybersecurity in cardiac implantable electronic devices. Expert Rev Med Devices 2019; 16: 437–44.

15. Ponemon Institute. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 2016.

16. Baylor Scott & White Medical Center. Important Notice Regarding a Data Security Incident; 2018.

17. Psykoterapiakeskus Vastaamo Psychotherapy Center. Vastaamo has become victim of a data system break-in and extortion., Psykoterapiakeskus Vastaamo; 2021.

18. INTERPOL.https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats; 2020.

19. Dullea E, Budke C, Enko P. Cybersecurity update: recent ransomware attacks against healthcare providers. Missouri Med 2020; 117: 533–4.

20. ·Digital Emblems: The Protection of Health Care Facilities in the Cyber Domain in the Age of Pandemics’, Opinio Juris, 28 October 2020.

21. Goodwin B. Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack computerweekly. Available at: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus; Last access on 11 March 2023

22. ·https://www.bloomberg.com/news/articles//parishospitals-target-of-failed-cyber-attack-authority-says/2021[42].

23. https://www.computing.co.uk/news/4012969/hospitalscoronavirus-ransomware /; Last Access on 11 March 2023.

24. https://www.computing.co.uk/news/4012969/hospitalscoronavirus-ransomware / Last Access on 11 March 2023.

25. Iaria A. Digital Emblems: The Protection of Health Care Facilities in the Cyber Domain in the Age of Pandemics', Opinio Juris, 28 October 2020.

26. IBM Security.Cost of a Data Breach Report. 2020. Available at: https://www.ibm.com/downloads/cas/QMXVZX6R

27. Busdicker M, Upendra P. The role of healthcare technology management in facilitating medical device cybersecurity. Biomed Instrum Technol 2017; 51: (6):19–25.

28. Bhuyan SS, Kabir U, Escareno JM, Ector K, Palakodeti S, Wyant D, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst 2020; 44(5):98.

29. Stack B. Here's How Much Your Personal Information Is Selling for on the Dark Web 2017. Available online at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web; Last access on 11 March 2023

30. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018; 113:48–52.

31. Bassett G, Hylender CD, Langlois P, Pinto A, Widup S. DBIR Data Breach Investigations Report 2008-2022. Available online at: https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf; Last access on 11 March 2023.

32. Sengupta K. *Isis-Linked Hackers Attack NHS Websites to Show Gruesome Syrian Civil War Images* (2017). Available online at: https://www.independent.co.uk/news/uk/ crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html (Last access on 11 March, 2023).

33. Langer SG. Cyber-security issues in healthcare information technology. J Dig Imag 2017; 30: 117–25.

34. https://www.internetsociety.org/

35. Peterson DC, Adams A, Sanders S, Sanford B. Assessing and addressing threats and risks to cybersecurity. Front Health Serv Manag 2018; 35:23–9.

36. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Sec 2020; 18: 228–31.

37. Spanaki EG, Bonomi S, Sfakianakis S, Santucci G, Lenti S, et al. Cyber-attacks and threats for healthcare - A multi-layer thread analysis. 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society Montreal, QC 2020; p: 5705–8.

INSTRUCTIONS FOR AUTHORS

The submitted manuscript must not be under consideration for publication in any other journal nor it may be already published in extenso or partly.

Annals of Nursing publishes **Original Research Articles, Reviews, Case Reports, Letters to Editor, Commentaries, and Editorials.**

The peer review is double blind with up to three reviewers.

The rights of the examinees must be protected by a mandatory informed consent. Patients' names must not appear in any part of the paper.

If any conflict of interest exists the authors have to make a detailed statement in the manuscript, before the list of references. If there is no conflict of interest the authors should state „ The authors declare no conflict of interest".

Manuscript submission

The papers should be submitted online through the journal website.

All manuscript pages must be numbered, starting from the front page. Use the Times Roman font 12, with left justification and double space. The maximum size of a paper, excluding tables and figures, depends on the type of submission: Original Research Article – 3500 words, Review Article – 5000 words, Case Report – 1500 words, Letter to Editor – 500 words, Commentary – 500 words. The number of tables and figures is limited to five and three, respectively.

Cover Letter should contain a statement that all co-authors have approved the content and submission of the paper and specify the role of each co-author in preparing the manuscript.

The corresponding author should make a statement about the conflict of interest. It should be stated that the manuscript has not been published nor is under consideration for publication elsewhere. The corresponding author should also explain why he/she thinks the paper should be published in the Annals of Nursing.

Front page contains the article title, the authors' full names, the authors' affiliations, word count, the number of tables, the number of figures, and the full name, email address and telephone of the corresponding author.

Abstract should have the size of up to 250 words, in a structured form, with subheadings: Background, Aim, Materials and Methods, Results and Conclusion.

The abstract of a narrative review should be written in one paragraph and in an unstructured form.

From 3-5 **Key words** follow the abstract.

Manuscript should be organized in six segments: Introduction, Materials and Methods, Results, Discussion, Acknowledgments and References.

References should be connected with the text using superscript figures by the order of mentioning.

If there are up to six authors mention them all. If there are more than six authors mention just the first three authors followed by “et al.”.

Here are the examples of citing:

Croxon L, Maginnis C. Evaluation of clinical teaching models for nursing practice. Nurse Education in Practice 2009; 9(4): 236–243.

Schreier M. Qualitative content analysis in practice. London: Sage; 2012.

Forrest-Lawrence P. Case study research. In: Liamputtong P. (Ed.), Handbook of research methods in health social sciences. Singapore: Springer, 2019; pp. 317–331.Statistik Austria . (2021) Healthcare personnel. Available[1]
at: https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/gesundheit/gesundheitsversorgung/personal_im_gesundheitswesen/index.html (accessed 08 July 2021) (in German)

Lercher P, de Coensel B, Dekoninck L, Bottldooren D. Alternative traffic noise indicators and its association with hypertension. Proceedings of the Euronoise 2018; May 27–31, 2018; Crete. [Madrid]: European Acoustic Assoc; Available
at http://www.euronoise2018.eu/docs/papers/80_Euronoise2018.pdf. Jointly published by the Hellenic Institute of Acoustics.

Tables

Tables should be uploaded separately and numbered. Please do not use vertical rules, while horizontal rules should be restricted to a minimum. Please indicate the place in the text where comes a table. Please do not use spaces to align columns in tables but use only one tab between each vertical column.

Figures

All illustrations should be provided electronically as separate graphic files (in GIF, TIF or JPEG format; 400 dpi) and not embedded in the text of the manuscript. Please number the figures. Please provide illustrations in the size that you want them to appear in the Journal. Legends for illustrations should be presented separately at the end of the manuscript and should be identified by number.

Publication Charge

For accepted papers a publication charge of 300 EUR will be applied prior to the start of publication process. Please visit www. annalsofnursing.org for payment.

CIP - Каталогизација у публикацији

Народна библиотека Србије, Београд

61

ANNALS of Nursing : a Quarterly International Journal : the Official Journal of the Medika College for Vocational Studies in Healthcare / editor in chief Goran Belojevic. - Vol. 1, issue 1 (2022)- . - - Belgrade : Medika College for Vocational Studies in Healthcare, 2022-(Belgrade : School Service Gajić). - 30 cm

Tromesečno. - Drugo izdanje na drugom medijumu:

Annals of Nursing (Online) = ISSN 2956-0306

ISSN 2956-0179 = Annals of Nursing
COBISS.SR-ID 78588681