

SEMINAR FOR PHYSICIANS SEMINAR ZA LEKARE U PRAKSI

CYBERSECURITY IN CLINICAL PRACTICE

SAJBER BEZBEDNOST U KLINIČKOJ PRAKSI

Daniel BJELICA¹, Gabriel-Stefan NAĐ² and Artur BJELICA²

ORCID NUMBER
Daniel Bjelica – 0009-0004-3486-9780

University Clinical Center of Vojvodina, Novi Sad
Radiology Center¹
Clinic for Gynaecology and Obstetrics²

Gabriel-Stefan Nađ – 0000-0002-9938-431X
Artur Bjelica – 0000-0002-1219-4936

Seminar for physicians
Seminar za lekare u praksi
UDK 614.2:[004.8:004.056.5
<https://doi.org/10.2298/MPNS2608215B>

Abstract

Introduction. The digitalisation of healthcare systems has led to a rapid proliferation of cybersecurity threats that directly affect everyday clinical practice. Electronic health records, networked medical devices, and telemedicine platforms have become integral to modern medicine while simultaneously representing potential attack surfaces. Clinicians make daily decisions with data security implications, and inadequate training leaves them particularly vulnerable. **Threats and vulnerabilities.** Ransomware attacks that paralyse hospital systems, phishing campaigns targeting clinical staff, attacks on medical *Internet of Things* devices, and software supply chain compromise are the most prevalent threats in the contemporary healthcare environment. Each carries direct consequences for patient safety and continuity of care. **Clinician roles and advanced technologies.** Clinical staff represent both the most frequent point of system compromise and the most important line of defence. Advanced technologies including artificial intelligence based threat detection, blockchain data integrity, and federated learning offer emerging solutions, but require strategic institutional commitment for successful deployment. **Conclusion.** Cybersecurity is not exclusively an information technology matter – it is an integral component of medical ethics and responsibility towards patients. Its routine integration into clinical practice requires education, clear institutional procedures, and adequate resources.

Key words: Computer Security; Clinical Medicine; Electronic Health Records; Confidentiality; Ethics, Medical; Patient Rights

Introduction

Modern clinical practice – from reproductive medicine to cardiology, oncology and primary care – depends fundamentally on digital infrastructure: electronic health record (EHR), picture archiving and communication systems (PACS), internet-connected infusion pumps, patient monitors, telemedicine platforms, and mobile health applications. Each of these systems represents both a clinical asset and a potential point of vulnerability. Healthcare organisations

Sažetak

Uvod. Digitalizacija zdravstvenih sistema donela je sa sobom brzo širenje sajber pretnji koje direktno utiču na svakodnevnu kliničku praksu. Elektronski zdravstveni kartoni, medicinski uređaji povezani na mrežu i telemedicinske platforme postali su sastavni deo savremene medicine, ali i potencijalne mete kibernetičkih napada. Klinički lekari svakodnevno donose odluke s implikacijama za bezbednost podataka, a nedostatak obuke iz ove oblasti čini ih posebno ranjivim. **Pretnje i ranjivosti.** Ransomware napadi koji parališu bolničke sisteme, phishing poruke usmerene ka kliničkom osoblju, napadi na medicinske *Internet of Things* uređaje i kompromitovanje lanaca snabdevanja softverom najčešće su pretnje u savremenom zdravstvenom okruženju. Svaka od ovih pretnji nosi direktne posledice po bezbednost pacijenata i kontinuitet zdravstvene zaštite. **Uloga kliničara i napredne tehnologije.** Klinički lekari predstavljaju i najčešću tačku prodora napada i najvažniju liniju odbrane. Napredne tehnologije poput veštačke inteligencije za detekciju pretnji, blockchain integriteta podataka i federativnog učenja nude nova rešenja, ali zahtevaju stratešku podršku institucija. **Zaključak.** Sajber bezbednost nije isključivo IT pitanje – ona je sastavni deo medicinske etike i odgovornosti prema pacijentima. Njena rutinska primena u kliničkoj praksi zahteva edukaciju, jasne institucionalne procedure i odgovarajuće resurse.

Ključne reči: sajber bezbednost; klinička medicina; elektronski zdravstveni kartoni; poverljivost; medicinska etika; prava pacijenata

are among the most attractive targets for malicious actors, owing to the high market value of patient data, the operational criticality of services that cannot be interrupted, and the comparatively immature state of security governance in many institutions [1].

The scale of the problem has grown consistently over the past decade. Annual survey data from HIMSS and Proofpoint-Ponemon document that a substantial majority of healthcare organisations experienced significant security incidents in the preceding twelve months [2,3]. Data breaches in health systems cause

✉ Corresponding author: Gabriel-Stefan Nađ, E-mail: gabrielnadj021@gmail.com, gabriel-stefan.nadj@mf.uns.ac.rs

Abbreviations

EHR	- electronic health record
PACS	- picture archiving and communication systems
GDPR	- General Data Protection Regulation
HIPAA	- Health Insurance Portability and Accountability Act
HITECH	- Health Information Technology for Economic and Clinical Health
AI	- artificial intelligence
IT	- information technology
IoMT	- Internet of Medical Things
MFA	- multi-factor authentication
EDR	- endpoint detection and response

damage on three simultaneous fronts: financial losses averaging millions of dollars per incident, reputational harm affecting patient trust, and direct clinical consequences, including delayed diagnoses, cancelled surgical procedures, and impaired access to medication records [2,3]. A systematic review published in *Cluster Computing* confirmed that breach-related disruption in healthcare is not merely a data governance concern but a patient safety issue of the first order [4].

Despite the severity of this threat, clinicians remain insufficiently prepared. Research conducted among practising physicians demonstrates that many are uncertain about their institutional security responsibilities and lack confidence in identifying or reporting incidents [5]. Training in cybersecurity across healthcare organisations remains ad hoc, inconsistently delivered, and rarely contextualised for clinical workflows [6].

Current threat landscape

Ransomware – malicious software that encrypts organisational data and demands payment for its release – represents the most operationally disruptive threat currently facing healthcare institutions. In clinical settings, the consequences are acute: patient management systems, laboratory results, radiology archives, and medication records can be rendered inaccessible for hours or days. Attacks of this type have been associated with measurable increases in patient mortality, particularly in emergency medicine and intensive care units where real-time data access is clinically indispensable. Both the HIMSS and Proofpoint-Ponemon reports rank ransomware among the top security concerns across health systems of all sizes [2,3], and the economic incentive for attackers is clear: healthcare organisations are less able to tolerate prolonged downtime than commercial enterprises, making them more likely to pay ransoms [4].

Phishing – the use of deceptive communications to extract credentials or deliver malware – remains the most common initial attack vector against healthcare systems [6,8]. Clinical staff are specifically vul-

nerable: high volumes of external communication, significant time pressure, and a professional culture that rewards rapid response all increase susceptibility. Healthcare systems are exposed to evolving cyber threats, including sophisticated phishing and social engineering attacks. At the same time, studies highlight persistent gaps in cybersecurity awareness and training among clinicians, which may hinder the identification of malicious communications [6,7].

The Internet of Medical Things (IoMT) – infusion pumps, defibrillators, implantable cardiac monitors, continuous glucose monitors, and bedside patient monitors connected to hospital networks – has created an attack surface that did not exist a decade ago. Many of these devices were designed before modern security standards existed, run legacy operating systems, and cannot receive software patches [7]. Deb et al., in a 2025 taxonomy of real-world IoMT attacks, documented incidents involving data interception, denial-of-service attacks targeting clinical devices, and, in adversarial research settings, unauthorised control of device function. ElSayed et al. proposed a lightweight adaptive machine-learning framework (CryptoDNA) for detecting distributed denial-of-service attacks in medical IoT environments, demonstrating that tailored artificial intelligence (AI)-based defences can address threats that generic security software does not cover [8]. Mohamadi et al. similarly showed that convolutional neural network models can detect known and novel threat types in IoMT networks at performance levels suitable for real-time deployment [9]. The clinical implication is unambiguous: a compromised medication-delivery device or patient monitor is not an IT problem – it is a patient safety incident.

Medical devices incorporating AI introduce a further category of risk. Mitra et al. demonstrated that AI-enabled devices can be targeted through adversarial manipulation of the underlying algorithms – not only through conventional network intrusion – and proposed a pre-market risk analysis framework extending security assessment to the behaviour of AI decision components [10]. Supply chain attacks, in which adversaries compromise a software vendor to gain simultaneous access to multiple downstream organisations, have been documented in healthcare IT. Argaw et al. identify insecure third-party interfaces as a primary structural vulnerability in hospital cybersecurity architectures [5,11].

Electronic health record security

Electronic health records are simultaneously the most operationally critical component of modern clinical workflow and among the most valuable tar-

gets for attackers. Health record data commands higher prices on illicit markets than financial data because a complete health record combines personal identifiers, diagnoses, medications, insurance information, and financial details that can be used for identity fraud, extortion, and fraudulent claims [1,4]. This economic reality drives targeted attacks specifically designed to exfiltrate health record data rather than encrypt it for ransom.

A quantitative study using structural equation modelling combined with artificial neural network analysis found that perceived cybersecurity risk is significantly associated with reduced trust in electronic health record systems and lower perceived performance among healthcare professionals [12]. These findings suggest that cybersecurity concerns may influence clinician engagement with digital health systems. Similarly, Arafa et al. report that perceived security plays an important role in shaping clinician acceptance and trust in emerging digital health technologies [1].

Core EHR security principles with direct relevance to clinical practice include: strong, unique credentials for each system supported by a password manager; multi-factor authentication (MFA) activated wherever available; minimum necessary access – each user accesses only data required for their current role; encryption of data in transit and at rest; and prompt reporting of anomalous system behaviour. Sharing login credentials with colleagues, even temporarily and in cases of clinical urgency, eliminates both technical access control and the audit trail that enables detection of unauthorised access.

The clinician's role in cybersecurity

Sociotechnical analyses consistently identify the human element as both the most frequent point of failure and the most important defensive resource in healthcare cybersecurity. Ewoh et al., in a 2025 scoping review published in the *Journal of Medical Internet Research*, propose a sociotechnical framework that integrates people, processes, and technology, placing clinicians at the centre of the security system rather than at its periphery [6]. The 2024 BMC qualitative study identified inadequate staff training and limited security awareness as key organisational risk factors, alongside broader systemic and governance-related challenges [13].

In day-to-day practice, clinicians make a continuous series of decisions with cybersecurity implications: whether to open an email attachment, use shared credentials for convenience, report a system anomaly, access patient data on a personal device.

Embedding security awareness into routine clinical behaviour – treating it as an element of professional competence alongside medication verification and infection control – is the most impactful intervention available at the individual level [5]. Prompt incident reporting is especially critical: unusual computer behaviour, unexpected system restarts, changes to the EHR interface appearance, unsolicited credential requests, and anomalous device behaviour can all indicate an active attack [5,7]. Alanazi's survey data show that a significant proportion of clinicians did not know where to direct a security report and doubted their report would receive a serious institutional response – a cultural failure with direct security consequences [5].

Advanced defensive technologies

AI-driven security systems can continuously monitor hospital networks, identify behavioural anomalies indicative of compromise, and isolate affected systems at speeds that manual oversight cannot match. The domain-specific machine-learning approaches demonstrated by ElSayed et al. and Mohammedi et al. illustrate how AI tools tailored to IoMT environments can address threat categories that generic security software fails to cover [8,9].

Blockchain technology has been proposed as a mechanism for ensuring the integrity and auditability of health records. The *Cluster Computing* systematic review identifies blockchain-based systems as among the most promising structural solutions for maintaining tamper-evident records of data access and modification – a property of particular value in environments where record authenticity is both a clinical and legal requirement [4]. Federated learning – a paradigm in which AI models are trained collaboratively across multiple institutions without patient data leaving each site – offers a path to more capable diagnostic algorithms while substantially reducing the security and privacy risks of centralised data aggregation [14].

The Zero Trust security model, endorsed by the World Economic Forum as a guiding architecture for healthcare cybersecurity, replaces the assumption that everything within a hospital network perimeter is trustworthy with continuous authentication and authorisation for every resource access event [15]. Ewoh et al. note that successful Zero Trust implementation requires alignment of technology, processes, and organisational culture – technical deployment alone is insufficient [6]. Regulatory frameworks such as GDPR in Europe and HIPAA/HITECH in the United States establish baseline requirements for data

protection and mandate breach notification obligations, with non-compliance potentially resulting in significant penalties. Healthcare cybersecurity bulletins from the U.S. HC3 highlight the relevance of these regulatory requirements amid ongoing cyber threats affecting the health sector [16].

Practical recommendations

For individual clinicians, credential management is the most immediately actionable area of responsibility. Strong, unique passwords for each system, with MFA enabled on every platform that supports it, are foundational; credentials must never be shared, and institutions should provide alternative emergency access protocols to avoid trading security for clinical urgency [2].

Alanazi reports variability in clinicians' awareness of cybersecurity threats and highlights uncertainty regarding institutional procedures for identifying and reporting suspicious communications, including potential phishing attempts [5].

Device-level security practices are widely recognised as important for reducing vulnerabilities in healthcare environments, particularly given the increasing attack surface associated with connected medical and information systems. From a user interaction perspective, perceived cybersecurity risks have also been shown to influence how healthcare professionals engage with electronic health record systems, highlighting the importance of secure system design and safe usage practices [7,12].

Studies highlight significant gaps in clinicians' cybersecurity awareness and uncertainty about institutional responsibilities, indicating the need for improved and context-sensitive cybersecurity education within healthcare environments. Both organisational and human-factor considerations are emphasised as important components of effective healthcare cybersecurity strategies [5,13]. Generic IT security content has limited impact; training using clinical scenarios – recognising a phishing message formatted as a laboratory result notification, understanding why credential sharing undermines both security and accountability – might produce greater and more durable behaviour change.

Technical measures should include network segmentation separating medical devices from administrative systems, regular vulnerability assessments, endpoint detection and response (EDR) deployment, and rigorously tested backup and recovery plans. IoMT devices warrant a dedicated institutional programme: central device inventories, network traffic monitoring, patch management where feasible, and

isolation of legacy devices that cannot be updated. Incident response plans must be documented, rehearsed with clinical leadership participation, and subject to systematic post-incident review.

Patient safety implications

The ultimate purpose of healthcare cybersecurity is to protect patients. Attacks that compromise data availability, disrupt device function, or immobilise clinical systems have direct consequences for diagnosis, treatment, and patient safety. Inaccessibility of allergy status, dosing errors attributable to device manipulation, and inability to order urgent investigations during system outages are documented outcomes of real-world ransomware attacks. Patient trust may also be eroded over the longer term. Data breaches have been associated in the literature with reduced patient confidence in healthcare systems, which may negatively influence openness in clinical communication.

Mitra et al. use a systems-theoretic framework to demonstrate that adversarial manipulation of machine learning models embedded in medical devices can lead to unsafe or erroneous outputs, highlighting limitations in conventional monitoring approaches for detecting such failures. These findings underscore the importance of robust safety and governance mechanisms for AI-enabled clinical decision support systems [10]. Along with these new possibilities, such systems also introduce new risks. Systems and models trained on single-centre datasets absorb and reproduce diagnostic habits and blind spots embedded in the environment. Such models can perpetuate single-institution biases when applied elsewhere [17].

Conclusion

Artificial intelligence offers transformative potential across many domains of clinical practice, from embryo selection in reproductive medicine to threat detection in cybersecurity, however, no technology is sufficient without the informed, vigilant clinician participation. The current threat environment continues to evolve: ransomware campaigns grow more sophisticated, Internet of Medical Things devices present novel attack surfaces, artificial intelligence is being weaponised, and supply chain compromises can affect entire regional health networks simultaneously. Advanced defensive technologies such as artificial intelligence-driven threat detection, blockchain integrity, federated learning and Zero Trust architecture are available and effective, but require strategic institutional commitment and adequate resources. Individual clinician behaviour remains indispensable

and cannot be substituted by technology: strong credential hygiene, vigilance against phishing, prompt incident reporting, and critical oversight of connected devices are professional responsibilities that belong

alongside medication safety and infection control in the daily practice of every clinician. The core message is straightforward: cybersecurity is a dimension of patient safety. It begins at the login screen.

References

1. Arafa A, Sheerah HA, Alsalamah S. Emerging digital technologies in healthcare with a spotlight on cybersecurity: a narrative review. *Information*. 2023;14(12):640.
2. Healthcare Information and Management Systems Society. 2024 HIMSS healthcare cybersecurity survey report [Internet]. Chicago: HIMSS; 2025 [cited 2026 May 15]. Available from: <https://cdn.sanity.io/files/sqo8bpt9/production/4f1c1968050411b8bf9335a187301881f9153b9f.pdf>
3. Ponemon Institute. Cyber insecurity in healthcare: the cost and impact on patient safety and care 2025 [Internet]. Sunnyvale (CA): Proofpoint; 2025 [cited 2026 May 15]. Available from: <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>
4. Nemec Zlatolas L, Welzer T, Lhotska L. Data breaches in healthcare: security mechanisms for attack mitigation. *Cluster Comput*. 2024;27(7):8639-54.
5. Alanazi AT. Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus*. 2023;15(10):e47026.
6. Ewoh P, Vartiainen T, Mantere T. Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: scoping review. *J Med Internet Res*. 2025;27:e75584.
7. Deb S, Lupu E, Drakakis EM, Bharath AA, Leung ZK, Ma GR, et al. Securing the Internet of Medical Things (IoMT): real-world attack taxonomy and practical security measures [Internet]. 2025 [cited 2026 May 15]. Available from: <https://arxiv.org/pdf/2507.19609>
8. ElSayed Z, Abdelgawad A, Elsayed N. CryptoDNA: a machine learning paradigm for DDoS detection in healthcare IoT, inspired by crypto jacking prevention models [Internet]. 2025 [cited 2026 May 15]. Available from: <https://arxiv.org/pdf/2501.18549>
9. Mohamadi A, Ghahramani H, Asghari SA, Aminian M. Securing healthcare with deep learning: a CNN-based model for medical IoT threat detection. In: 19th Iranian Conference on Rad je primljen 2. VI 2026. Recenziran 19. VI 2026. Prihvaćen za štampu 24. VI 2026. BIBLID.0025-8105:(2026):LXXIX:7-8:215-219.
- Intelligent Systems (ICIS); 2024 Oct 23-24; Sirjan, Iran. Sirjan: Sirjan University of Technology, 2024. p. 168-73.
10. Mitra G, Hallajiyani M, Kim I, Dharmalingam AP, Elnawawy M, Iqbal S, et al. Systems-theoretic and data-driven security analysis in ML-enabled medical devices [Internet]. 2025 [cited 2026 May 15]. Available from: <https://arxiv.org/pdf/2506.15028>
11. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, et al. Cybersecurity of hospitals: challenges and risk mitigation. *BMC Med Inform Decis Mak*. 2020;20:146.
12. Ala'a M, Ramayah T, Al-Sharafi MA. Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: a multi-analytical SEM-ANN approach. *Technol Soc*. 2024;77:102592.
13. Burke W, Stranieri A, Oseni T, Gondal I. The need for cybersecurity self-evaluation in healthcare. *BMC Med Inform Decis Mak*. 2024;24(1):133.
14. Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. *NPJ Digit Med*. 2020;3:119.
15. World Economic Forum. A rise in healthcare cyberattacks calls for zero trust [Internet]. Geneva: World Economic Forum; 2023 [cited 2026 May 15]. Available from: <https://www.weforum.org/stories/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/>
16. U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center. HC3 Healthcare: Cybersecurity Bulletin [Internet]. 2023 [cited 2026 May 15]. Available from: <https://www.hhs.gov/sites/default/files/hc3-healthcare-cybersecurity-bulletin-q1-2023.pdf>
17. Fogt F. The illusion of diagnostic agreement - institutional bias as a hidden force in modern medicine. *Med Pregl*. 2025;78(5-8):127-31.