Received 20 March 2025
Revised 4 May 2025
Accepted 23 May 2025

Who should do what to help mitigate cyber threats in health care: narrative review of practical approaches and actionable recommendations

Hrvoje Belani
Directorate for e-Health, Republic of Croatia Ministry of Health, Zagreb, Croatia and
Department of Computer Science and Technology, VERN' University, Zagreb, Croatia, and
Kristina Fišter
Department of Medical Statistics, Epidemiology and Medical Informatics, Andrija Štampar School of Public Health, University of Zagreb School of Medicine, Zagreb, Croatia

Abstract

Purpose – Cyber attacks on health care are ubiquitous, increasingly sophisticated and can cost lives. The health care sector has been lagging behind other industries in digital transformation, including investments in cybersecurity. Stakeholders' awareness of their own responsibilities and those of others in mitigating cyber threats is often limited.
Design/methodology/approach – For this narrative literature review, on 30 April 2025, we searched without date, language or geographical restrictions PubMed, Web of Science, Scopus, IEEE Xplore and EBM Reviews for journal articles that reported practical approaches and actionable recommendations to improve cybersecurity in health care. Our initial search returned 720 articles; following supplementary searches and screening, a total of 45 relevant documents were included.
Findings – Described are the expected roles of key stakeholders in mitigating cyber threats, from governments and lawmakers to health care managers, information technology experts and clinical providers. Health care organisations must step up investments in cybersecurity. Each organisation must develop and implement a strong cybersecurity strategy. State-of-the-art approaches include training to resist phishing, as well as the use of the principle of least privilege for user and administrative access, traffic monitoring tools, endpoint detection and response technologies, along with timely security patching. Zero trust architecture is gaining in relevance and use. Best approaches to balancing cybersecurity with minimal disruption of workflows include user-centric solutions that utilise multi-factor authentication combined with one-time passwords, biometrics or smart cards.
Originality/value – A comprehensive overview of practical approaches and actionable recommendations for improving cybersecurity in health care, presented by key stakeholders' roles, delineating state-of-the-art in this fast-moving field.

Keywords Cybersecurity, Health care, Data breach, Cyber attack, Ransomware, Recommendations
Paper type Literature review

Introduction

Cyber attacks on health care are a growing threat globally (Lancet, 2024), causing operational and financial difficulties but also threatening patients' safety and well-being. Attackers' motivations include financial or political gain and the potential to take lives in a form of cyber warfare (Coventry and Branley, 2018). Materialised threats have affected hospitals, insurance

International Journal of Health Governance
Vol. 30 No. 3, 2025
pp. 282-292
Emerald Publishing Limited
e-ISSN: 2059-464X
p-ISSN: 2059-4631
DOI 10.1108/IJHG-03-2025-0030

Competing interests: We have reviewed the journal's policy and have no competing interests to declare.

companies, information technology (IT) vendors and others (Ghafur *et al.*, 2019; Daly, 2022; Antoniuk, 2024; Reuters, 2025), resulting in postponed or cancelled appointments, shutdown networks and information systems, patient transfers to other facilities and processes reverted to paper-based mode. Attacks vary, from phishing (sending false e-mails containing malicious content) through malware (malicious software capable of spreading and causing harm to computing and data resources) to ransomware (blackmailing malware that cryptographically locks-out access to resources and data, asking for ransom, usually in cryptocurrency).

Many cyber attacks manifest as "advanced persistent threats", conducted by organised groups using sophisticated techniques (OCIO, 2023). A targeted entity is attacked persistently until the group's goal is achieved, which can last months (CW Jobs, 2016). Health care is increasingly targeted because of growing vulnerabilities, caused by burgeoning applications and services, interconnected and used by numerous users (Lancet, 2024). Widespread are outdated and legacy technologies that do not support novel protection approaches. A sizable increase in threats was seen during the COVID-19 pandemic, prompting the WHO to call for (mondiale de la Santé, 2024) improved efforts in the prevention and detection of threats, which however can only be mitigated rather than prevented entirely. Data breaches are a matter of "when" rather than "if" for health care organisations (Lancet, 2024). It has become necessary for cybersecurity to be incorporated into business strategies (Zerlang, 2022). For over a decade, the average cost of data breaches globally has been higher in health care than in any other industry (Ukyab and Beato, 2024).

Cybersecurity in health care organisations is often viewed as the responsibility of IT departments; however, other stakeholders have key roles to play (WHO, 2024). Preventing and mitigating threats is the proverbial cat-and-mouse game, with the system as secure as its weakest link. We have therefore set out to review available literature for practical approaches and actionable recommendations to mitigating cybersecurity threats in health care.

Methods

We have conducted comprehensive literature searches from database inception to 30th April 2025 of PubMed, Web of Science, Scopus, IEEE Xplore and the EBM Reviews via Ovid (including the American College of Physicians (ACP) Journal Club, Database of Abstracts of Reviews of Effects, Cochrane Central Register of Controlled Trials, Health Technology Assessment, Cochrane Database of Systematic Reviews, National Health Service Economic Evaluation and Cochrane Methodology Register), without language or geographical restrictions. Search strings were tailored to the distinctive search structures of the included databases (see Appendix, Supplementary data S1: Search strategy), comprising the terms cybersecurity, data security, information security, security vulnerability, data breach, cyberattack, ransomware; hospital, health system, health care organisation, health information system, patient privacy, electronic health record; best practice, risk management, strategy, recommendation, technology, framework. This was supplemented by non-systematic reference and citation searches.

We included journal articles that described practical approaches and actionable recommendations to improving cybersecurity in health care. Excluded were articles that reported on specific settings, such as field hospitals or organ donation procurement, or specific technologies such as mHealth and wearables aimed solely at patients and the public, telemedicine, telemonitoring and telemetry, as well as clinical photographs and other images, biomedical signals, production of biopharmaceuticals and drug development, storage of genomic sequence data and secondary data use infrastructures. Conference papers, patents and retracted articles were also excluded.

We used Rayyan (Ouzzani *et al.*, 2016) for handling the search results, detecting duplicates and screening articles for relevance based on titles and abstracts, followed by a full-text screening of selected studies. One reviewer with a Master of Science degree in information sciences (KF) conducted the searches and screening of the articles, with the other reviewer (HB) checking this work and both initiating discussions as deemed needed. We synthesised the studies according to major stakeholders responsible for cybersecurity in health care. Given the

narrative review design and the characteristics of the available evidence, a formal quality appraisal of the included studies was not performed. No written protocol existed for this narrative review. In choosing the optimal type of knowledge synthesis method most suitable for the purpose of this review, we consulted Right Review, a web-based decision support tool (Amog *et al.*, 2022). We are unaware of formal reporting guidelines or checklists for narrative, traditional literature reviews, so have conducted and reported the study in line with the best available resources (Booth *et al.*, 2021; Gasparyan *et al.*, 2011; Parker and Sikora, 2022) and broadly followed the PRISMA guideline for systematic reviews where considered relevant (Page *et al.*, 2021). The PRISMA flowchart and a glossary of technical terms are available in the Appendix as Supplementary data S2 and S3, respectively.

Results

Our initial search returned 720 articles, of which 67 were deleted as duplicates and 144 were selected for full-text retrieval and screening. Of these, 27 were included in the review. Through supplemental searches, we identified 18 additional relevant documents for inclusion. There were no disagreements between the reviewers that would require adjudication by a third party.

Governments and lawmakers

In the first overview of the state of cybersecurity in the European Union (ENISA, 2024), the European Union Agency for Cybersecurity called for policymakers to enhance the understanding of sectorial specificities and needs, as well as improve the level of cybersecurity maturity, in the health care sector *inter alia* and in line with relevant legislation such as the NIS2 Directive (EUR-Lex, 2022), the Cyber Resilience Act (EUR-Lex, 2024) and the Cyber Solidarity Act (EUR-Lex, 2025). It is up to governments and lawmakers to develop and implement national cybersecurity strategies, policies and frameworks, including for health care.

A cybersecurity framework is a set of guidelines for enterprises to follow to better identify, detect and respond to cyber-attacks (Syafrizal *et al.*, 2020; Adnan *et al.*, 2024). It includes guidance on how to prevent or recover from attacks through a set of standards, methodologies, procedures and processes. The United States of America's National Institute of Standards and Technology (NIST) Cybersecurity Framework is often used, which has been developed following President Barack Obama's executive order (NIST, 2013), together with other available frameworks such as the International Organization for Standardization and the International Electrotechnical Commissions (ISO/IEC) 27001, Health Information Trust Alliance - Common Security Framework (HITRUST), European Union's General Data Protection Regulation (GDPR), United States' Health Insurance Portability and Accountability Act (HIPAA), Control Objectives for Information and Related Technologies from ISACA® (COBIT®), NIST's National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE), Committee of Sponsoring Organizations – the Treadways Commissions (COSO) and others (Syafrizal *et al.*, 2020).

It is up to policymakers to ensure that all stakeholders work towards the common goal of data protection (Pool *et al.*, 2024). This can be facilitated by establishing appropriate communication channels and collaborations between IT departments, health executives, providers of clinical care, vendors and other technology providers, insurers and patient groups, as well as by providing adequate funding for these activities. Information sharing between stakeholders has been recommended in order to build resilience (Argaw *et al.*, 2020). Patients and the public must be engaged and informed about their rights and the measures that have been put in place to protect their data (Pool *et al.*, 2024). Continued monitoring to detect and respond to incidents in a coordinated way, including ransomware attacks and data breaches, can be set up at the national level (CISA, 2025).

Educational programs must be created and funded to train the medical informatics workforce (Fišter *et al.*, 2019), including specialists in cybersecurity, who are in growing demand. Finally, health care reform has been proposed as a means to curb cyber attacks (Farringer, 2019). Governments have been warned that, until there are changes to the health care infrastructure,

there is a danger that security measures will be applied piecemeal, with the most vexing challenges left inadequately addressed. Therefore, a "comprehensive health care reform that includes cybersecurity not just as a thought, but as a purpose and goal of system redesign" has been called for to most efficiently and effectively address cybersecurity risk (Farringer, 2019).

Health care executive leaders

Health care executives are responsible for fostering a positive and inclusive workplace culture, prioritising the work-life balance of employees, as well as for fostering a strong cybersecurity culture that holds security a top priority (Subramanian *et al.*, 2024). It is up to institutional leaders to develop fair and accessible policies, regularly update them and design frameworks for keeping patients and employees informed, ensure quality internal and external communications, as well as compliance with data protection laws.

Organisation top executives must prioritise the strengthening of IT and security departments (Pool *et al.*, 2024), addressing cybersecurity in a preventative and proactive way, with strong IT infrastructure as the foundation (Argaw *et al.*, 2020). It is important to have a designated cybersecurity team, led by a Chief Information Security Officer (Kruse *et al.*, 2017b) or another designated person if this role does not exist in the organisation, such as the chief of IT. The roles and responsibilities should be clearly assigned within the team. In addition, there should be a clear agreement at the organisation level on what constitutes a reportable incident and when to escalate (Argaw *et al.*, 2020).

Executives and board members should implement comprehensive data protection strategies and allocate sufficient resources to IT and security departments; this includes ensuring adequate education and training for all staff, as well as promoting a culture of responsible use of data (Pool *et al.*, 2024; Farringer, 2019; Kruse *et al.*, 2017a). Oversight of cybersecurity risk management must be incorporated into governance and a risk communication plan developed as part of incident response support in case of realised data breaches or cyber attacks (Subramanian *et al.*, 2024).

IT leaders and staff

IT leaders, in roles such as chief information officers, chief information security officers, data protection officers and IT/security managers, together with IT staff should prioritise fostering a culture of data security and shared responsibility within the organisation (Pool *et al.*, 2024; Clarke and Martin, 2024). This includes advocating for education and training programs, with an aim to prevent health care workers' noncompliant behaviour and lack of awareness, which facilitates data breaches (Arafa *et al.*, 2023). Scenario-based training and periodic assessments can facilitate compliance (Pool *et al.*, 2024).

Beyond ensuring compliance with existing regulations, standards and frameworks, IT leaders must create and implement cybersecurity strategies that encompass well-considered solutions for the variety of potential threats, including prevention, detection, response and recovery mechanisms (Zandona and Thompson, 2017; Arafa *et al.*, 2023). Taken into account when formulating information security policies should be organisational characteristics, such as its size as well as the size of the IT department, and security resources (Pool *et al.*, 2024). This should include the development of incident response protocols and business continuity plans, to promptly address and manage data breaches or realised threats; these protocols should be regularly tested, exercised and stored offline (Argaw *et al.*, 2020).

Protocols also need to be put in place to address data protection failures in third-party sources, which includes the establishment of robust business associates' assessment and monitoring processes (Pool *et al.*, 2024). Data protection officers, together with IT leaders and staff, should assess and enhance data protection measures in third-party sources by establishing reasonable criteria for external partners and business associates. Cloud service providers, for example, must be compliant with relevant certifications and requirements, with solid approaches to role-based access, network security mechanisms, data encryption, digital

signatures and access monitoring (Rodrigues *et al.*, 2013). mHealth app developers should contribute to the prevention of breaches by ensuring adequate data protection while presenting the apps in mobile app markets (Pool *et al.*, 2024).

The IT/security department should implement effective access controls and monitoring mechanisms to mitigate noncompliant behaviour among health care workers (Pool *et al.*, 2024). Techniques to protect electronic health records from unauthorised access and use of data span technical, physical and administrative safeguards, although no approach will thwart spurious or accidental breaches with absolute certainty (Kruse *et al.*, 2017b). Technical access control (synonymous with media controls, entity authentication, encryption, firewall, audit trails, virus checking, or packet filtering), whether role-based, attribute-based, or identity-based, aims to enable user access to the patient information only as needed. A provider only has access to the patient data for those patients they are caring for. Another example is clerks only having access to administrative data.

Firewalls are considered essential, but each organisation must assess its needs, budget and potential threats, both internal and external, before deciding which type of firewall to opt for (Sichkar and Pavlova, 2023). A four-phase firewall security strategy has been described, encompassing service control, direction control, user control and behaviour control (Wikina, 2014). Failure to follow these best practices has been associated with a number of reported cases of data breaches (Kruse *et al.*, 2017b).

Use of cryptography is another essential method of technical access control. Encryption must be used while data are in transit, at rest on storage devices and during backups (Arafa *et al.*, 2023; Subramanian *et al.*, 2024). Cloud computing can be a solution for some organisations to keep costs at bay while maintaining cryptography protections (Kruse *et al.*, 2017b), yet cloud-based electronic health record solutions may also aggravate security concerns, for which various remedies have been proposed (Sahi *et al.*, 2021; Alenoghena *et al.*, 2022; Wang *et al.*, 2019; Gupta *et al.*, 2024); therefore, it is important that IT staff ensure that best security practices are followed by the technology providers, in order to mitigate potential threats. In addition, some settings report use of tokens (Wang *et al.*, 2022) or masking of data (Martínez *et al.*, 2013).

Best practice procedures must ensure updating all systems, including devices and medical equipment, patching vulnerabilities, use of a product stewardship framework to continually improve and innovate procedures (Lewis, 2019), and implementing secure communication technologies such as Internet Relay Chat channels. Installation and regular updating of antivirus software are used successfully in most settings (Kruse *et al.*, 2017b). It is possible to implement tools for continuous security monitoring, whereby threats are identified and reported as they happen, enabling a response to potential incidents in real-time (Naghib *et al.*, 2025; Harris, 2024; Arafa *et al.*, 2023). Some also use radio frequency identification to control access, by storing data within tags or restricting access to tags to specific devices. When patients access their data, digital signatures coupled with decryption ensure privacy, with some emerging solutions available for safe delegated authorisation, important in cases of patient incapacitation (Joshi *et al.*, 2021). Furthermore, usernames and passwords assigned by a system administrator can be used to establish role-based access controls, which protect from internal breaches or threats. Multi-factor authentication is increasingly used to control access and is considered best practice (Subramanian *et al.*, 2024; Arafa *et al.*, 2023) for all administrative and privileged users, and preferably for all users (Argaw *et al.*, 2020). To implement multi-factor authentication while preserving minimally disturbed workflow, the use of one-time passwords, biometrics, or smart cards has been suggested (Moriarty, 2021).

Physical access control (synonymous with physical security, workstation security, assigned security responsibility, media controls/access cards, or physical safeguard) is a technique that controls physical access to resources to ensure that only authorised people can physically enter appropriate parts of premises (Kruse *et al.*, 2017b). For example, patients only have access to those clinics or wards where they are seen; or, clinical providers do not have access to the server room, i.e. their access cards do not open those doors. Finally, administrative safeguards (synonymous with risk analysis and management, system security evaluation, personnel

chosen for certain roles, contingency, business continuity and disaster recovery planning) are policies, practices and procedures put in place to regularly check for vulnerabilities and continually improve security in an organisation.

IT departments will make sure to follow and implement relevant standards and ensure the use of secure networks like virtual local area networks; also, to regularly back up data in order to ensure continuity and recovery from potential ransomware attacks or data loss incidents, organise ongoing employee security awareness training and phishing simulations, carry out routine internal audits and risk assessments, conduct privacy impact assessments and ensure transparency in data processing, as well as keep abreast of mature and emerging technologies (Alenoghena *et al.*, 2022; Arafa *et al.*, 2023), such as zero trust architecture or tools based on artificial intelligence, applying them as appropriate (Subramanian *et al.*, 2024; Williams *et al.*, 2020). Zero trust is increasingly used for the superior security it affords, as it denies access to applications and data by default, as well as for its potential to prevent medical errors (Sood *et al.*, 2024). Best practices also include network segmentation, with hospital networks separated into different areas and strict access controls between them, which helps contain potential breaches and limit the lateral movement of attackers, reducing the impact of a realised cyber attack (Arafa *et al.*, 2023).

Artificial intelligence has been viewed as a major threat (Mohsin Khan *et al.*, 2025), as illustrated by the chatbot WotNot data breach (Cluley, 2024), but also as a major potential contributor to making health information systems more secure (Messinis *et al.*, 2024; Shankar *et al.*, 2024; Ali *et al.*, 2025; Seh *et al.*, 2021). One approach has been user and entity behaviour analytics (Shashanka *et al.*, 2016), which offers automated detection of anomalous behaviour utilising machine learning. Other cybersecurity technologies, all with their advantages and disadvantages, include blockchain, authentication schemes, federated learning, differential privacy and homomorphic encryption (Messinis *et al.*, 2024).

In the age of Internet-of-medical-things, bring-your-own-device, increasingly remote physicians' work and patient-collected data through monitoring and other devices, managing endpoint security has become the factor that most contributes to an organisation's overall cybersecurity (Clarke and Martin, 2024). The IT staff must ensure regular updates and patches for the devices that connect to health care networks, as well as the application of endpoint detection and response technologies, from diversified vendors if possible (Hira, 2025). As new devices are added, IT staff should ensure integration with current systems and cybersecurity plans; related protocols should be easily accessible to staff responsible for procurement of the devices, so they can determine whether prospective vendors will meet the requirements (Clarke and Martin, 2024).

Information sharing and collaboration with industry peers, government agencies and cybersecurity organisations enhance the collective ability to defend against cyber threats (Arafa *et al.*, 2023).

Providers of clinical care

Ensuring system security and data privacy is a shared responsibility, which includes clinical end-users of IT technology (Clarke and Martin, 2024). Security measures can be disruptive to clinical workflows, therefore balancing risks and functionality is a key challenge. Clinicians should participate in making decisions about cybersecurity solutions, which must be user-centric. Security breaches can compromise the quality of care, therefore clinicians should treat protection of patient data as an integral part of providing high-quality care (Pool *et al.*, 2024).

Regular training of all clinical staff has often been emphasised as one of the most important security measures to implement (Ewoh and Vartiainen, 2024; Kruse *et al.*, 2017a; Clarke and Martin, 2024). In such programs, covered are topics like strong password management, recognising phishing attempts, secure data handling and device security (Clarke and Martin, 2024). An employee falling for a phishing scam has been among the most common methods of realised threats (Yeo and Banfield, 2022). Good practices include requiring users to frequently change personal passwords and passwords not including meaningful names or dates to the individual (Kruse *et al.*, 2017b). Users should also remember to log out of the system after each use.

Physicians and other clinical staff must strictly adhere to data access protocols, ensuring that only authorised people have access to patient data (Pool *et al.*, 2024). Full compliance with security policies and conscientious attending of regular training is vital for mitigating cyber threats. Active engagement in cybersecurity awareness programs helps to stay updated on protection measures and best practices. Any witnessed privacy violation, suspicious security activity, or behaviour noncompliant with the organisation's security policies should be vigilantly reported to IT staff. A curious sneak peek into a record of a patient for whom the clinician has not provided care constitutes a data breach; about half of all data breaches are internal (Coventry and Branley, 2018). In addition to following best practices as outlined above, providers of clinical care can also be leaders in their professional societies and in their communities, supporting calls for legislative and other actions to improve cyber protection (Rizzoli, 2021).

Conclusions

Health care cybersecurity is a shared responsibility. We have outlined the expected roles of key stakeholders, from governments and lawmakers to health care managers, IT experts and clinical providers. Awareness and acceptance of own responsibilities, diligent following of the best practices, as well as awareness of other stakeholders' actions towards the shared goal of a secure system is of key importance. With 'advanced persistent threats' ubiquitous, prevention of cyber threats has become synonymous with mitigating the consequences of realised attacks, while internal breaches remain the target of ethical, legal and technical safeguards.

As a paramount, health care must step up investments in cybersecurity as well as sharing of information and international cooperation. Each organisation must develop and implement a strong cybersecurity strategy, considering its vulnerabilities, capacity for resilience and readiness. Even organisations with limited resources can and should implement well-equipped dedicated cyber incident response teams (DeVoe and Rahman, 2015). State-of-the-art approaches include building capacity for resisting phishing attempts throughout the organisation, as well as using the principle of least privilege for user and administrative access, traffic monitoring tools and endpoint detection and response technologies, along with timely security patching. Zero trust architecture is gaining in relevance and use (Kindervag, 2010; Bradley, 2023; NSA, 2024). Best approaches to balancing cybersecurity with minimal disruption to workflows include user-centric solutions that utilise multi-factor authentication combined with one-time passwords, biometrics, or smart cards. With growing requirements for secondary use and data sharing, novel approaches will be needed to keep the data safe (Riou *et al.*, 2025).

Due to the wide scope and limited space, in this review, we could not delve deeper into individual approaches and technologies, especially emerging ones. Some principles are only briefly mentioned, such as the use of a product stewardship framework (3M, 2025), therefore readers are encouraged to explore further. In addition, a large proportion of our search results (102/720) were articles addressing blockchain. While the recent proliferation of the literature on this technology is a clear testament to an upsurge in interest and optimism (Alshar'e *et al.*, 2024), at times seemingly pedestalling it as a silver-bullet panacea, future work is needed to critically explore the advantages and drawbacks of blockchain as well as its utility in health care cybersecurity, beyond ensuring nonrepudiation. Another limitation of our review is that we have not included other stakeholders that have roles to play in contributing to cybersecurity in health care, such as organisational legal and human resources departments, insurers, media, patients, visitors and the public.

References

3M (2025), "Sustainability: explore environmental, social, and governance impact | 3M", available at: https://www.3m.com/3M/en_US/sustainability-us/ (accessed 10 March 2025).

Adnan, M., Kutafina, E. and Beyan, O. (2024), "Cybersecurity frameworks in healthcare data: short literature review", *Studies in Health Technology and Informatics*, Vol. 316, pp. 301-302, doi: 10.3233/SHTI240403.

Alenoghena, C.O., Onumanyi, A.J., Ohize, H.O., Adejo, A.O., Oligbi, M., Ali, S.I. and Okoh, S.A. (2022), "eHealth: a survey of architectures, developments in mHealth, security concerns and solutions", *International Journal of Environmental Research and Public Health*, Vol. 19 No. 20, 13071, doi: 10.3390/ijerph192013071.

Ali, S.M., Razzaque, A., Yousaf, M. and Shan, R.U. (2025), "An automated compliance framework for critical infrastructure security through artificial intelligence", *IEEE Access*, Vol. 13, pp. 4436-4459, doi: 10.1109/ACCESS.2024.3524496.

Alshar'e, M., Abuhmaidan, K., Ahmed, F.Y.H., Abualkishik, A., Al-Bahri, M. and Yousif, J.H. (2024), "Assessing blockchain's role in healthcare security: a comprehensive review", *Informatica*, Vol. 48 No. 22, pp. 1-16, doi: 10.31449/inf.v48122.6155.

Amog, K., Pham, B., Courvoisier, M., Mak, M., Booth, A., Godfrey, C., Hwee, J., Straus, S.E. and Tricco, A.C. (2022), "The web-based 'Right Review' tool asks reviewers simple questions to suggest methods from 41 knowledge synthesis methods", *Journal of Clinical Epidemiology*, Vol. 147, pp. 42-51, doi: 10.1016/j.jclinepi.2022.03.004.

Antoniuk, D. (2024), "LockBit claims cyberattack on Croatia's largest hospital", *The Record*, July, available at: https://therecord.media/lockbit-claims-cyberattack-croatia-hospital

Arafa, A., Sheerah, H.A. and Alsalamah, S. (2023), "Emerging digital technologies in healthcare with a spotlight on cybersecurity: a narrative review", *Information*, Vol. 14 No. 12, p. 640, doi: 10.3390/info14120640.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A. (2020), "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks", *BMC Medical Informatics and Decision Making*, Vol. 20 No. 1, p. 146, doi: 10.1186/s12911-020-01161-7.

Booth, A., Sutton, A., Clowes, M. and Martyn-St James, M. (2021), *Systematic Approaches to a Successful Literature Review*, 3rd ed., SAGE Publications, London.

Bradley, T. (2023), "The 'godfather of zero trust' joins illumio", *Forbes*, available at: https://www.forbes.com/sites/tonybradley/2023/09/25/the-godfather-of-zero-trust-joins-illumio/ (accessed 28 February 2025).

CISA (2025), "Healthcare and public health cybersecurity | CISA", available at: https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare (accessed 7 March 2025).

Clarke, M. and Martin, K. (2024), "Managing cybersecurity risk in healthcare settings", *Healthcare Management Forum*, Vol. 37 No. 1, pp. 17-20, doi: 10.1177/08404704231195804.

Cluley, G. (2024), "AI chatbot startup WotNot leaks 346,000 files, including passports and medical records", *Hot for Security*, December, available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/ai-chatbot-startup-wotnot-leaks-346-000-files-including-passports-and-medical-records (accessed 9 March 2025).

Coventry, L. and Branley, D. (2018), "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward", *Maturitas*, Vol. 113, pp. 48-52, doi: 10.1016/j.maturitas.2018.04.008.

CW Jobs (2016), "Cyber crime timeline", 10 August, available at: http://www.cwjobs.co.uk/careers-advice/it-glossary/cyber-crime-timeline (accessed 9 March 2025).

Daly, P. (2022), "Writing on a curved surface' the operational response to the cyber-attack on the Irish health service", *Medecine de Catastrophe - Urgences Collectives*, Vol. 6 No. 4, pp. 275-277, doi: 10.1016/j.pxur.2022.10.002.

DeVoe, C. and Rahman, S. (2015), "Incident response plan for a small to medium sized hospital", *arXiv Preprint*, arXiv:1512.00054.

ENISA (2024), "2024 report on the state of the cybersecurity in the union | ENISA".

EUR-Lex (2022), "EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex", available at: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng (accessed 7 March 2025).

EUR-Lex (2024), "Regulation - 2024/2847 - EN - EUR-Lex", available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (accessed 7 March 2025).

EUR-Lex (2025), "Regulation - EU - 2025/38 - EN - EUR-Lex", available at: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng (accessed 7 March 2025).

Ewoh, P. and Vartiainen, T. (2024), "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review", *Journal of Medical Internet Research*, Vol. 26, e46904, doi: 10.2196/46904.

Farringer, D.R. (2019), "Maybe if we turn it off and then turn it back on again? Exploring health care reform as a means to curb cyber attacks", *Journal of Law Medicine and Ethics*, Vol. 47 No. 4, pp. 91-102, doi: 10.1177/1073110519898046.

Fišter, K., Belani, H., Relić, D. and Erceg, M. (2019), "Biomedical informatics workforce in Croatia: qualitative analysis of teachers' opinions on needs and employment opportunities", *Studies in Health Technology and Informatics*, Vol. 264, pp. 1921-1922, doi: 10.3233/SHTI190714.

Gasparyan, A.Y., Ayvazyan, L., Blackmore, H. and Kitas, G.D. (2011), "Writing a narrative biomedical review: considerations for authors, peer reviewers and editors", *Rheumatology International*, Vol. 31 No. 11, pp. 1409-1417, doi: 10.1007/s00296-011-1999-3.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019), "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *NPJ Digital Medicine*, Vol. 2 No. 1, pp. 1-7, doi: 10.1038/s41746-019-0161-6.

Gupta, L.M., Samad, A., Garg, H. and Shah, K. (2024), "An effective metaheuristic based dynamic fine grained data security framework for big data", *Wireless Personal Communications*, Vol. 137 No. 4, pp. 2441-2468, doi: 10.1007/s11277-024-11506-4.

Harris, C. (2024), "The top 8 continuous security monitoring tools", *Expert Insights*, 7 May, available at: https://expertinsights.com/insights/the-top-continuous-security-monitoring-tools/ (accessed 10 March 2025).

Hira, R. (2025), "Developing highly resilient architecture for critical systems to mitigate operational risks", *International Journal of Scientific Engineering and Science*, Vol. 9 No. 1, pp. 30-35.

Joshi, M., Joshi, K. and Finin, T. (2021), "Delegated authorization framework for EHR services using attribute-based encryption | IEEE journals & magazine | IEEE Xplore", *IEEE Transactions on Services Computing*, Vol. 14 No. 6, pp. 1612-1623, doi: 10.1109/TSC.2019.2917438.

Kindervag, J. (2010), "Build security into your network's DNA: the zero trust network architecture", Forrester Research, available at: http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (accessed 28 February 2025).

Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017a), "Cybersecurity in healthcare: a systematic review of modern threats and trends", *Technology and Health Care*, Vol. 25 No. 1, pp. 1-10, doi: 10.3233/THC-161263.

Kruse, C.S., Smith, B., Vanderlinden, H. and Nealand, A. (2017b), "Security techniques for the electronic health records", *Journal of Medical Systems*, Vol. 41 No. 8, p. 127, doi: 10.1007/s10916-017-0778-4.

Lancet (2024), "Cyberattacks on health care—a growing threat", *Lancet*, Vol. 403, 10441, p. 2263, doi: 10.1016/S0140-6736(24)01074-2.

Lewis, D.H. (2019), "A strategic approach to product stewardship 2", *PM World Journal*, Vol. VIII No. VII.

Martínez, S., Sánchez, D. and Valls, A. (2013), "A semantic framework to protect the privacy of electronic health records with non-numerical attributes", *Journal of Biomedical Informatics*, Vol. 46 No. 2, pp. 294-303, doi: 10.1016/j.jbi.2012.11.005.

Messinis, S., Temenos, N., Protonotarios, N.E., Rallis, I., Kalogeras, D. and Doulamis, N. (2024), "Enhancing internet of medical things security with artificial intelligence: a comprehensive review", *Computers in Biology and Medicine*, Vol. 170, 108036, doi: 10.1016/j.compbiomed.2024.108036.

Mohsin Khan, M., Shah, N., Shaikh, N., Thabet, A., Alrabayah, T. and Belkhair, S. (2025), "Towards secure and trusted AI in healthcare: a systematic review of emerging innovations and ethical challenges", *International Journal of Medical Informatics*, Vol. 195, 105780, doi: 10.1016/j.ijmedinf.2024.105780.

mondiale de la Santé, O. and World Health Organization (2024), "Examining the threat of cyber-attacks on health care during the COVID-19 pandemic = Menace liée aux cyberattaques dans le secteur de la santé pendant la pandémie de COVID-19", *Weekly Epidemiological Record = Relevé Épidémiologique Hebdomadaire*, Vol. 99 No. 4, pp. 25-37.

Moriarty, K.M. (2021), "Why are authentication and authorization so difficult?", *Center for Internet Security*, 18 October, available at: https://www.cisecurity.org/blog/why-are-authentication-and-authorization-so-difficult (accessed 18 March 2025).

Naghib, A., Gharehchopogh, F.S. and Zamanifar, A. (2025), "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities", *Artificial Intelligence Review*, Vol. 58 No. 4, p. 114, doi: 10.1007/s10462-024-11101-w.

NIST (2013), "Cybersecurity framework", *Inside NIST*, 12 November, available at: https://www.nist.gov/cyberframework (accessed 7 March 2025).

NSA (2024), "NSA releases maturity guidance for the zero trust network and environment pillar", *National Security Agency/Central Security Service*, available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3695223/nsa-releases-maturity-guidance-for-the-zero-trust-network-and-environment-pillar/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3695223%2Fnsa-releases-maturity-guidance-for-the-zero-trust-network-and-environment-pillar%2F (accessed 28 February 2025).

OCIO (2023), "Types of cyber threat actors that threaten healthcare. Threat brief ID# 202306081300", *Health Sector Cybersecurity Coordination Center (HC3)*, June, available at: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Ouzzani, M., Hammady, H., Fedorowicz, Z. and Elmagarmid, A. (2016), "Rayyan-a web and mobile app for systematic reviews", *Systematic Reviews*, Vol. 5 No. 1, p. 210, doi: 10.1186/s13643-016-0384-4.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P. and Moher, D. (2021), "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", *BMJ, British Medical Journal Publishing Group*, Vol. 372, p. n71, doi: 10.1136/bmj.n71.

Parker, R. and Sikora, L. (2022), "Literature reviews: key considerations and tips from knowledge synthesis librarians", *Journal of Graduate Medical Education*, Vol. 14 No. 1, pp. 32-35, doi: 10.4300/JGME-D-21-01114.1.

Pool, J., Akhlaghpour, S., Fatehi, F. and Burton-Jones, A. (2024), "A systematic analysis of failures in protecting personal health data: a scoping review", *International Journal of Information Management*, Vol. 74, 102719, doi: 10.1016/j.ijinfomgt.2023.102719.

Reuters (2025), "UnitedHealth says hack at tech unit impacted 190 million people", 25 January.

Riou, C., Azzouzi, M.E., Hespel, A., Guillou, E., Coatrieux, G. and Cuggia, M. (2025), "Ensuring general data protection regulation compliance and security in a clinical data warehouse from a university hospital: implementation study", *JMIR Medical Informatics*, Vol. 13 No. 1, e63754, doi: 10.2196/63754.

Rizzoli, P. (2021), "10 things clinicians need to know about healthcare cyberattacks", *Bulletin of the Croatian Society for Medical Informatics*, Vol. 27 No. 2, pp. 9-14.

Rodrigues, J.J.P.C., de la Torre, I., Fernández, G. and López-Coronado, M. (2013), "Analysis of the security and privacy requirements of cloud-based electronic health records systems", *Journal of Medical Internet Research*, Vol. 15 No. 8, e186, doi: 10.2196/jmir.2494.

Sahi, A., Lai, D. and Li, Y. (2021), "A review of the state of the art in privacy and security in the eHealth cloud", *IEEE Access*, Vol. 9, pp. 104127-104141, doi: 10.1109/ACCESS.2021.3098708.

Seh, A., Al-Amri, J., Subahi, A., Agrawal, A., Kumar, R. and Khan, R. (2021), "Machine learning based framework for maintaining privacy of healthcare data", *Intelligent Automation and Soft Computing*, Vol. 29 No. 3, pp. 697-712, doi: 10.32604/iasc.2021.018048.

Shankar, D.D., Azhakath, A.S., Khalil, N., Sajeev, J., Mahalakshmi, T. and Sheeba, K. (2024), "Data mining for cyber biosecurity risk management – a comprehensive review", *Computers and Security*, Vol. 137, 103627, doi: 10.1016/j.cose.2023.103627.

Shashanka, M., Shen, M.-Y. and Wang, J. (2016), "User and entity behavior analytics for enterprise security", *In 2016 IEEE International Conference on Big Data (Big Data)*, pp. 1867-1874, doi: 10.1109/BigData.2016.7840805.

Sichkar, M. and Pavlova, L. (2023), "A short survey of the capabilities of next generation firewalls", *Computer Science and Cybersecurity*, No. 1, pp. 28-33, doi: 10.26565/2519-2310-2023-1-02.

Sood, N., Parlapalli, R., Sharma, P. and Kashyap, R. (2024), "Application of zero trust model in preventing medical errors", *Frontiers in Health Services*, Vol. 4, 1453804, doi: 10.3389/frhs.2024.1453804.

Subramanian, H., Sengupta, A. and Xu, Y. (2024), "Patient health record protection beyond the health insurance portability and accountability Act: mixed methods study", *Journal of Medical Internet Research*, Vol. 26, e59674, doi: 10.2196/59674.

Syafrizal, M., Selamat, S.R. and Zakaria, N.A. (2020), "Analysis of cybersecurity standard and framework components", *International Journal of Communication Networks and Information Security*, Vol. 12 No. 3, doi: 10.17762/ijcnis.v12i3.4817.

Ukyab, K.T. and Beato, F. (2024), "Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key", *World Economic Forum*, 1 February, available at: https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/ (accessed 6 March 2025).

Wang, X., Bai, L., Yang, Q., Wang, L. and Jiang, F. (2019), "A dual privacy-preservation scheme for cloud-based eHealth systems", *Journal of Information Security and Applications*, Vol. 47, pp. 132-138, doi: 10.1016/j.jisa.2019.04.010.

Wang, K., Chen, C.-M., Tie, Z., Shojafar, M., Kumar, S. and Kumari, S. (2022), "Forward privacy preservation in IoT-enabled healthcare systems", *IEEE Transactions on Industrial Informatics*, Vol. 18 No. 3, pp. 1991-1999, doi: 10.1109/TII.2021.3064691.

WHO (2024), "WHO director-general's remarks at meeting of the UN security council on threats posed by ransomware attacks against hospitals and other health-care facilites and services", 8 November, available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks (accessed 6 March 2025).

Wikina, S.B. (2014), "What caused the breach? An examination of use of information technology and health data breaches", *Perspectives in Health Information Management*, Vol. 11, Fall, p. 1h.

Williams, C.M., Chaturvedi, R. and Chakravarthy, K. (2020), "Cybersecurity risks in a pandemic", *Journal of Medical Internet Research*, Vol. 22 No. 9, e23692, doi: 10.2196/23692.

Yeo, L.H. and Banfield, J. (2022), "Human factors in electronic health records cybersecurity breach: an exploratory analysis", *Perspectives in Health Information Management*, Vol. 19, Spring, p. 1i.

Zandona, D.J. and Thompson, J.M. (2017), "Going beyond compliance: a strategic framework for promoting information security in hospitals", *The Health Care Manager*, Vol. 36 No. 4, pp. 364-371, doi: 10.1097/HCM.0000000000000189.

Zerlang, J. (2022), "Why cybersecurity should be part of any business strategy", *Forbes*, available at: https://www.forbes.com/councils/forbestechcouncil/2022/11/21/why-cybersecurity-should-be-part-of-any-business-strategy/ (accessed 17 March 2025).

Supplementary material
The supplementary material for this article can be found online.

Corresponding author
Kristina Fišter can be contacted at: kristina.fister@snz.hr