© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723336

From Attack to Recovery: An Integrated Cyber Resilience Framework for Healthcare Institutions

DR. GULSHAN KUMAR[1], SAHARSH GERA[2], JITENDER[3]
[1] *Associate Professor, Rawal Institute of Management, Faridabad*
[2,3] *Assistant Professor, Institute of Innovation in Technology & Management, New Delhi*

Abstract- ***Hospitals have become frequent targets of ransomware, phishing and data theft, and an outage can endanger patients as well as records. This review traces how attacks on healthcare organisations since 2016 turn into clinical harm and examines how strong the evidence is for the measures proposed against them. English-language literature was searched mainly in PubMed, and 29 records were synthesised thematically. Phishing-enabled ransomware and unpatched legacy systems account for most reported incidents, from WannaCry in 2017 to the Irish HSE attack in 2021, and their consequences include cancelled procedures, diverted emergencies and medication-safety risk during downtime. Mandatory annual awareness modules have not been shown to reduce successful phishing, whereas repeated simulation with feedback and rehearsed downtime drills look more promising, although most evidence comes from single sites. Only a small minority of organisations were reported to go beyond basic monitoring. The paper proposes a Prevent–Prepare–Respond–Recover framework that treats clinical downtime competence as a security control, and calls for outcome-based evaluation of drills, training and legacy-device management.***

Index Terms- ***Cyber-resilience, downtime procedures, healthcare cybersecurity, patient safety, phishing, ransomware***

I. INTRODUCTION

Clinical care now runs on digital systems: electronic medical records (EMR), telemedicine and connected diagnostic and therapeutic devices. As hospitals abandon paper, safe care depends on those systems staying available [1], [2]. The same connectivity enlarges the attack surface, because interlinked devices and portals allow a single breach to spread across departments [3], [2].

Two features make the sector attractive to attackers. Health records combine identifiers, financial data and clinical detail whose value persists, and an identity, unlike a payment card, cannot be re-issued [4], [5]. In addition, an interruption of care puts hospitals under exceptional pressure to pay [6]. Sector surveys report very high attack rates [7], yet many incidents are never disclosed [8].

An attack on a hospital differs from one on most other organisations because it can harm patients directly: records become inaccessible, equipment may fail, and laboratory results are delayed [1], [2]. Earlier reviews have mapped attack trends [9], hospital risks and mitigation [10], [11], and sociotechnical weaknesses [12]. What is missing is an integrated account that follows an attack from its entry point to its clinical consequences and then to the measures that keep care going during an outage.

This paper re-analyses the corpus assembled in the systematic review of Chima et al. [13], reorganises it around that pathway, grades the evidence behind each class of measure, and derives a resilience framework. It asks:

1) Which attack vectors and incidents have characterised healthcare cyber-attacks since 2016?
2) How do such attacks become clinical, operational and organisational harm?
3) Which preventive, preparedness and response measures are proposed, and how strong is the evidence for them?
4) What integrated framework and research agenda follow?

II. BACKGROUND

A. Definition

A healthcare cyber-attack is used here to mean any deliberate, malicious attempt to compromise patient privacy, healthcare data, or operational systems such as medical equipment, EMR and hospital networks [14], [1]. Security aims to protect the confidentiality, integrity and availability of health data [8]; in a clinical setting availability matters at least as much as

confidentiality, since an inaccessible record can halt treatment.

B. Historical development

Attacks on health organisations began to appear in the early 2000s [15]. In 2015 roughly 113 million health records were reported compromised, 78.8 million of them in one attack [16]. Later years brought more capable tools and a larger attack surface [17], and the COVID-19 pandemic accelerated both telemedicine and exposure [6], [17].

C. Why the sector remains a target

Health organisations hold data of high monetary and intelligence value, including identity data, financial details, protected health information and research data [4]. Durable data behind comparatively weak defences is an appealing combination [9], and stolen records have been reported to fetch a premium over payment-card credentials on dark-web markets [18], [5]. Attackers may also expect larger payments where disruption threatens public life, and medical innovation may attract state-sponsored actors [6].

III. REVIEW METHOD

A structured, qualitative design was used. An initial scoping search in Google Scholar for "hospital cyberattack" was followed by systematic searching in PubMed, chosen for its biomedical scope and free full-text access, although PubMed and Google Scholar are known to differ in retrieval performance [19]. The strings were "healthcare cyberattack technology", "healthcare data breaches" and "hospital cyberattack prevention case study". Records were eligible if they were in English, published from 2016 onward, and concerned cyber-attacks, cybersecurity or resilience in healthcare organisations; purely technical IT records without a healthcare context were excluded. Twenty-nine records were retained (Fig. 1). Data on incidents, vectors, consequences and measures were extracted and synthesised thematically.

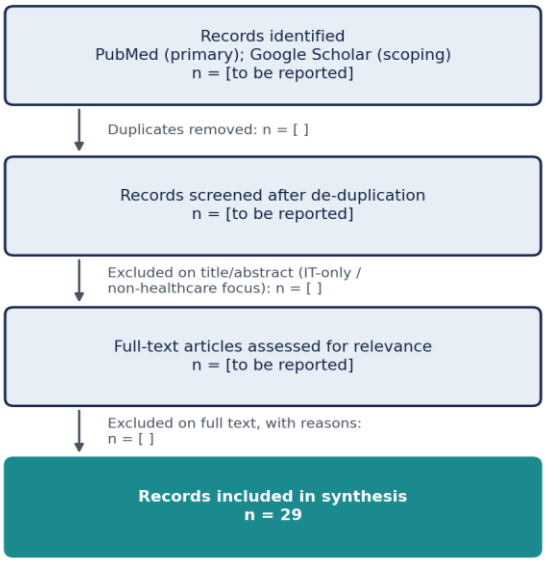

Fig. 1. Flow of records through identification, screening, eligibility and inclusion. Bracketed counts are to be completed from the search log; 29 is the reported size of the corpus.

IV. FINDINGS

A. The incident landscape

Table I and Fig. 2 list the principal incidents. Three patterns stand out. The mechanisms are mostly ordinary: unpatched software, human-operated ransomware and phishing-led intrusions. National responses tend to follow major incidents rather than precede them; France announced €350 million for healthcare cybersecurity after a run of ransomware attacks, and Germany made IT security mandatory in health as digitisation advanced [6]. And the volume of activity can be huge: Spanish health organisations were reported to face over 50,000 attacks in 2020, about 430 per week per organisation, rising to 626 in January 2021 [6].

TABLE I
Selected healthcare cyber-incidents

Incident	Vector and reported consequences	Ref.
WADA (2016)	Unauthorised access; athletes' medical records published; motive unclear.	[20]

Incident	Vector and reported consequences	Ref.
WannaCry (May 2017)	Ransomware exploiting unpatched systems; about one third of NHS trusts affected; surgeries and appointments cancelled; some emergency departments shuttered; >200,000 computers in >150 countries. An audit judged it unsophisticated and preventable with basic IT practice.	[6], [21], [22]
Düsseldorf Univ. Hospital (Sep 2020)	Ransomware on 30 servers; ambulance diverted; one death reported in connection with the diversion.	[6]
Spain (2020–21)	Phishing through to ransomware; >50,000 attacks reported in 2020.	[6]
France (2020)	27 major attacks reported; ransomware at Villefranche hospital.	[6]
HSE Ireland (14 May 2021)	Human-operated Conti ransomware; most services shut down; facilities offline.	[6]

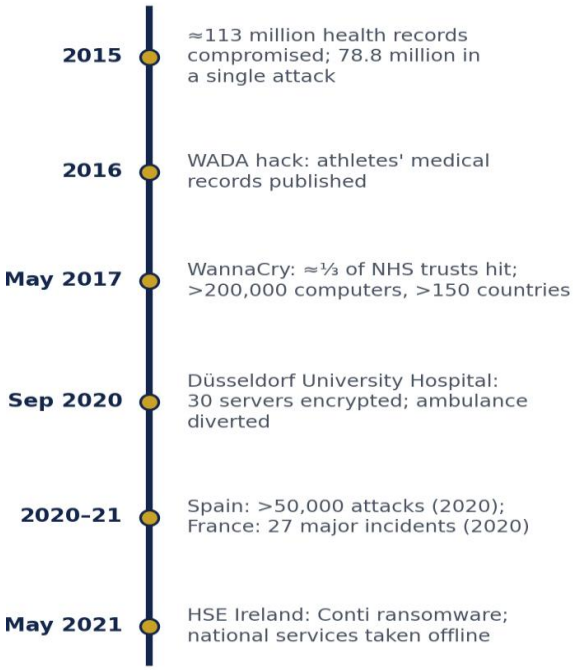

Fig. 2. Timeline of selected incidents and sector indicators reported in the reviewed literature, 2015–2021.

B. Attack vectors and structural weaknesses

Social engineering and ransomware. Most breaches in the corpus began with phishing or ransomware, which exploit human factors, often called the weakest link, as well as technical flaws [9], [23]. Legacy systems. Studies report that a large majority of organisations and devices depend on old platforms such as Windows XP that no longer receive security updates or routine offline backups [24], [12], [21]. This was the weakness WannaCry exploited on more than 200,000 computers in over 150 countries [21]. Devices and telehealth. Medical devices and telehealth platforms lack standardised security protocols, so one compromised component can expose connected networks [25]. An outdated device can give access to the EMR or allow false results to reach physicians [11], and telehealth sessions can be intercepted when patients' own devices are poorly protected [11], [25].

C. From attack to clinical harm

Fig. 3 synthesises the pathway from vector to consequence. Because hospital systems are interdependent, one entry point can produce system-wide effects: unavailable records, unreliable devices such as infusion pumps, pacemakers, ventilators and

imaging equipment, and delayed laboratory results [1], [2]. Untrustworthy devices can force cardiac, stroke and trauma services to close to admissions [26]. Beyond the ward, healthcare is reported to spend more than other industries on resolving breaches and faces class-action litigation and reputational damage [1], [27].

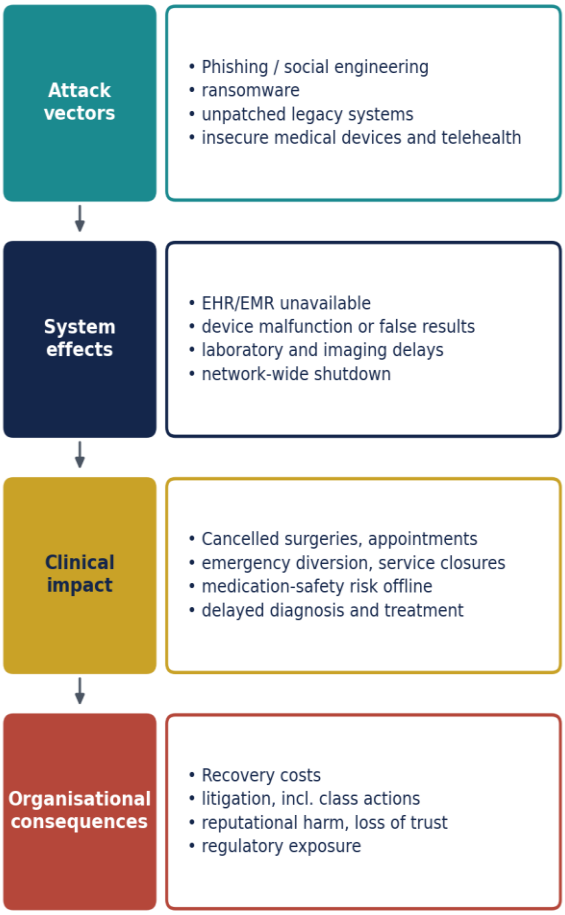

Fig. 3. Pathway from attack vector to system effects, clinical impact and organisational consequences.

A second, less visible pathway concerns clinical skills. Since EMR adoption, doctors have moved away from conventional ways of recording, ordering and prescribing. During downtime they may lack decision support, drug–interaction alerts and selectable dosages, and clinical pharmacists become essential for excluding allergies and interactions [28]. The literature therefore argues that clinical judgement must take precedence over such aids, and that print-outs and paper processes should be practised in advance [2].

D. Organisational preparedness

Preparedness looks uneven. An industry report found that over a quarter of healthcare organisations had low security maturity, without recommended threat-detection capabilities, and that only about 3% went beyond basic monitoring [29]. Downtime protocols usually cover scheduled outages and are ill suited to prolonged offline operation [1]. Fig. 4 shows the indicators; since they come from different populations they are illustrative, not a single comparable series.

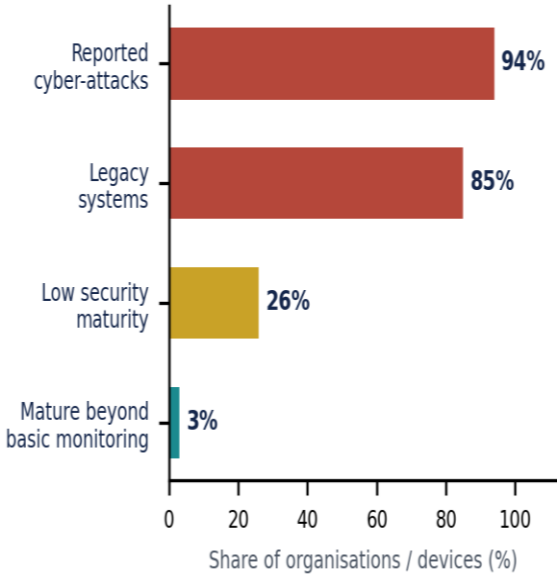

Fig. 4. Selected sector indicators: reported cyber-attacks (SANS, via Zarour et al.) [7]; legacy systems [21]; low maturity and mature capability [29]. Secondary citations; verify primary sources before quantitative use.

E. Measures and the strength of evidence

Table II grades the evidence for the main measures. Because most sources are single-site case studies, simulations, expert reviews or grey literature, only three levels are used: low (opinion or conceptual argument), moderate (observational or single-site evaluation) and emerging (prototype or early technology).

TABLE II
Preventive and preparedness measures

Measure	Evidence	Caveat and source
Dedicated security staff	Low	Rests on industry commentary [25].

Measure	Evidence	Caveat and source
Mandatory annual training	Moderate (negative)	Not shown to cut successful phishing; fatigue and low retention suggested [30].
Phishing simulation with feedback	Moderate	Mostly single-site studies [31], [23], [28].
Downtime drills and paper practice	Moderate	ICU and hospital simulations; patient outcomes not measured [32], [2].
Patching; retiring or isolating legacy systems	Moderate	Post-incident analyses [21], [22]; some devices cannot be updated.
Multi-factor authentication and access policies	Low–moderate	Usability trade-offs [1]; current guidance does not support forced periodic password changes absent evidence of compromise [33].
Security-by-design devices	Low	Conceptual [24].
Blockchain-secured EHR	Emerging	Prototypes and reviews; cost limits adoption [34], [35], [27].
Look-alike domain registration	Low	Single proposal [31].

Two points deserve emphasis. First, the weak record of mandatory annual training contrasts with more encouraging results for repeated, realistic simulation, suggesting that format and frequency matter more than the mere existence of training [30], [31]. In an ICU simulation, participants who felt less stress communicated better and responded faster [32]. Second, the corpus recommends running drills as often as fire drills, with department-specific downtime protocols nested within the hospital structure [31], [2].

V. PROPOSED FRAMEWORK

Fig. 5 groups the measures into four phases that a hospital board and a clinical department can both act on. The phases map onto the incident-response lifecycle in the literature (planning and preparation; detection; analysis; containment and eradication; recovery; post-incident activity).

Prevent combines technical hygiene with dedicated expertise: security staff distinct from IT operations, timely patching, retirement or isolation of legacy systems, multi-factor authentication, and procurement of devices with security built in. Prepare is where the framework departs most from conventional security models, because it treats clinical downtime competence as a control: downtime manuals, stocks of approved paper charts and protocols, recurrent drills, phishing simulation and downtime practice in medical curricula. Respond follows the incident response plan; in standard practice the network is shut down and privileged credentials changed, then security staff inspect connected devices to find and fix the breach before relaunch, while departments activate downtime protocols. Recover covers verified restoration, secure relaunch and a post-incident review that feeds back into plans, drills and training.

Four enablers cut across the phases: a culture in which individual lapses are recognised as entry points and reporting is easy; leadership that treats cybersecurity as part of patient safety; regulation and standards; and, as an emerging option, blockchain-secured EHR. Security cannot guarantee that attacks are prevented, but sound practice can reduce their severity.

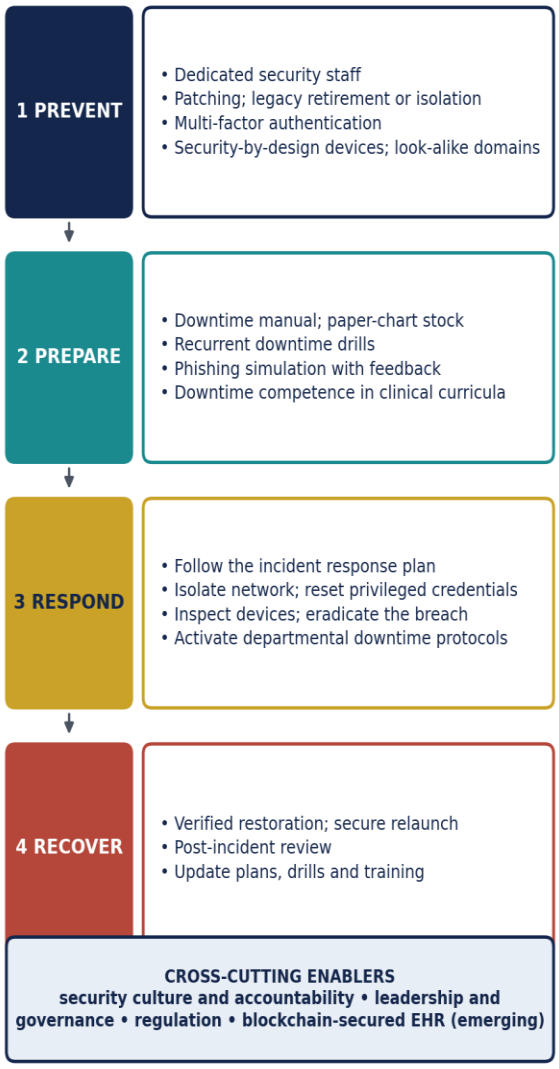

Fig. 5. Prevent–Prepare–Respond–Recover framework with cross-cutting enablers, synthesised from the reviewed literature.

VI. DISCUSSION

A. Comparison with prior work and implications

The findings agree with earlier reviews that identify phishing, ransomware and outdated infrastructure as recurring enablers. The added contribution is to connect these vectors to the clinical pathway of harm and to treat downtime competence as part of the security architecture. WannaCry illustrates the point: an attack judged unsophisticated disrupted a national health service with real cyber capability, because of small lapses in basic practice.

For hospital leaders, the results support dedicated security staff, systematic patching and a legacy-asset register that supports explicit risk–benefit decisions where devices cannot be updated. For educators, they support downtime scenarios and paper-based practice in curricula and simulation programmes. For security teams, they favour repeated phishing simulation with timely feedback over check-box modules, balanced against usability so that busy clinicians are not driven to workarounds. For regulators, the pattern of reactive investment argues for proactive standards for devices and telehealth platforms.

B. Research agenda

1) Controlled or quasi-experimental studies of drills and simulation that measure patient-safety and recovery outcomes rather than perceptions.
2) Comparative effectiveness of training formats and frequencies, including why mandatory modules fail.
3) Risk–benefit methods for devices whose software cannot be updated.
4) Independent clinical evaluation of blockchain-based EHR, including cost and interoperability.
5) Transparent incident reporting to counter under-reporting and support incidence estimates [8].
6) Studies in resource-constrained health systems, which are under-represented in the corpus.

C. Limitations

PubMed was the principal database, so relevant work indexed elsewhere may be missing; adding Scopus, Web of Science, IEEE Xplore and ACM Digital Library would widen coverage. The corpus is English-only and starts in 2016. Much incident data comes from grey literature and secondary reporting, several statistics are second-hand, and no formal risk-of-bias tool was applied, so the grades in Table II are indicative. The synthesis is narrative, the framework is not empirically validated, and the threat landscape changes quickly.

VII. CONCLUSION

Healthcare cyber-attacks are a patient-safety problem as much as a data-protection problem. A small set of recurring weaknesses, namely phishing, ransomware, unpatched legacy systems and insecure devices, is enough to cancel procedures and divert emergencies. The framework proposed here is intended as a working

tool for hospital boards, clinical educators and security teams, and its central practical message is that downtime should be rehearsed as routinely as fire evacuation. Its central scientific message is that outcome-based evidence is now needed to show which measures actually protect patients.

REFERENCES

[1] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," *Front. Digit. Health*, vol. 4, Art. no. 862221, 2022, doi: 10.3389/fdgth.2022.862221. Frontiers

[2] B. Abbou, B. Kessel, and M. Ben Natan, "When all computers shut down: The clinical impact of a major cyber-attack on a general hospital," *Front. Digit. Health*, vol. 6, Art. no. 1321485, 2024, doi: 10.3389/fdgth.2024.1321485. Frontiers

[3] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Appl. Clin. Inform.*, vol. 7, no. 2, pp. 624–632, 2016, doi: 10.4338/ACI-2016-04-SOA-0064. Thieme

[4] J. Riggi, "The importance of cybersecurity in protecting patient safety," *American Hospital Association*, 2021. American Hospital Association

[5] C. M. Williams, R. Chaturvedi, R. D. Urman, et al., "Cybersecurity risks in a pandemic," *J. Med. Internet Res.*, vol. 22, no. 9, Art. no. e23692, 2020, doi: 10.2196/23692. JMIR

[6] D. Rees, "Cyber-attacks in healthcare: The position across Europe," *Pinsent Masons*, 2021. Pinsent Masons

[7] M. Zarour, et al., "Ensuring data integrity of healthcare information in the era of digital health," *Healthc. Technol. Lett.*, 2021, doi: 10.1049/htl2.12008. Wiley

[8] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: How safe are we?," *BMJ*, vol. 358, Art. no. j3179, 2017, doi: 10.1136/bmj.j3179. BMJ

[9] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018, doi: 10.1016/j.maturitas.2018.04.008. Crossref

[10] S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacey, et al., "Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, Art. no. 146, 2020, doi: 10.1186/s12911-020-01161-7. Springer

[11] E. A. Al-Qarni, "Cybersecurity in healthcare: A review of recent attacks and mitigation strategies," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, 2023, doi: 10.14569/IJACSA.2023.0140513. Crossref

[12] P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review," *J. Med. Internet Res.*, vol. 26, Art. no. e46904, 2024, doi: 10.2196/46904. JMIR

[13] R. O. Chima, T. O. Odeyemi, A. Ojo, E. O. Ahmadu, and D. E. Akinbinu, "Cyberattacks on healthcare systems and the need for cybersecurity: A systematic literature review," *J. Int. Rev. Res. Stud.*, vol. 1, no. 10, pp. 1–15, 2026, doi: 10.66104/ptx1wg79.

[14] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," *Internet Things*, vol. 20, Art. no. 100615, 2022, doi: 10.1016/j.iot.2022.100615. Crossref

[15] M. Glick, "Cyberattacks on health care are rising – but many hospitals aren't prepared," *Discover Magazine*, 2021.

[16] HIPAA Journal, "Healthcare cybersecurity," 2022. HIPAA Journal

[17] S. Duguin, "If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition," *World Economic Forum*, 2021. World Economic Forum

[18] A. Zistler, "Hacking healthcare IT in 2016: Lessons the healthcare industry can learn from the OPM breach," *Medical Design & Outsourcing*, 2016.

[19] S. Z. Shariff, S. A. Bejaimal, J. M. Sontrop, et al., "Retrieving clinical evidence: A comparison of PubMed and Google Scholar for quick clinical

searches," *J. Med. Internet Res.*, vol. 15, no. 8, Art. no. e164, 2013, doi: 10.2196/jmir.2624. JMIR

[20] "Wiggins and Froome medical records released by 'Russian hackers'," *BBC News*, 2016.

[21] S. Ghafur, S. Kristensen, K. Honeyford, et al., "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *npj Digit. Med.*, vol. 2, Art. no. 98, 2019, doi: 10.1038/s41746-019-0161-6. Nature

[22] National Audit Office, "Investigation: WannaCry cyber attack and the NHS," HC 414, 2018.

[23] A. Wright, S. Aaron, and D. W. Bates, "The big phish: Cyberattacks against U.S. healthcare systems," *J. Gen. Intern. Med.*, vol. 31, no. 10, pp. 1115–1118, 2016, doi: 10.1007/s11606-016-3741-z. Springer

[24] M. Busdicker and P. Upendra, "The role of healthcare technology management in facilitating medical device cybersecurity," *Biomed. Instrum. Technol.*, vol. 51, no. s6, pp. 19–25, 2017, doi: 10.2345/0899-8205-51.s6.19. PubMed

[25] S. Alder, "Healthcare data breach statistics," *HIPAA Journal*, 2024.

[26] American Medical Association, "Cybersecurity in medical practice," *AMA Ed Hub*. [Online]. Available: [URL, year and access date to be verified]

[27] A. Kumar, A. K. Singh, and I. Ahmad, "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol. 22, no. 15, Art. no. 5921, 2022, doi: 10.3390/s22155921.

[28] K. K. Haase, M. M. Whitworth, and K. Yalamanchili, "Clinicians' experiences and reflections from a health system cyberattack," *J. Am. Coll. Clin. Pharm.*, vol. 4, no. 6, pp. 738–742, 2021, doi: 10.1002/jac5.1423. Wiley

[29] Kroll, "The state of cyber defense: Diagnosing cyber threats in healthcare," 2024. Kroll

[30] W. J. Gordon, A. Wright, R. J. Glynn, et al., "Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system," *J. Am. Med. Inform. Assoc.*, vol. 26, no. 6, pp. 547–552, 2019, doi: 10.1093/jamia/ocz005. PubMed

[31] F. Rizzoni, S. Magalini, A. Casaroli, et al., "Phishing simulation exercise in a large hospital: A case study," *Digit. Health*, vol. 8, 2022, doi: 10.1177/20552076221081716. SAGE

[32] M. Willing, C. Dresen, E. Gerlitz, et al., "Behavioral responses to a cyber-attack in a hospital environment," *Sci. Rep.*, vol. 11, Art. no. 19352, 2021, doi: 10.1038/s41598-021-98576-7. Nature

[33] P. A. Grassi, J. L. Fenton, E. M. Newton, et al., "Digital identity guidelines: Authentication and lifecycle management," *NIST Special Publication 800-63B*, 2017, doi: 10.6028/NIST.SP.800-63b. NIST

[34] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, 2016.

[35] Hasselgren, K. Kralevska, D. Gligoroski, et al., "Blockchain in healthcare and health sciences: A scoping review," *Int. J. Med. Inform.*, vol. 134, Art. no. 104040, 2020, doi: 10.1016/j.ijmedinf.2019.104040. Crossref