Telemedicine International

Telemedicine International 2026; 2:799
doi:10.4081/tmi.2026.799

Cybersecurity in healthcare as a clinical competency: a conceptual proposal informed by recent evidence

Paolo Sossai,[1,2,3] Nicola Fabbri[4]

[1]Editor-in-Chief, Telemedicine International; [2]Director, Department of Health, Maxi-Emergencies and Disaster International School (MEDIS), Modena; [3]President, Central Medical Commission, Italian Alpine Club (CAI), Milan; [4]Director of Sales, Marketing & Business Development, Alchimie Digitali S.r.l., Modena, Italy

Abstract

The progressive digitalization of healthcare delivery and the widespread adoption of telemedicine have significantly expanded the attack surface of clinical infrastructures.
Recent evidence shows that cybersecurity incidents do not result solely in informational or reputational harm, but are associated with measurable adverse clinical outcomes, including excess in-hospital mortality during ransomware attacks.
In this editorial, we argue that healthcare cybersecurity should be recognized, at both the operational and governance levels, as a clinical competency, on par with hand hygiene, radiation protection, and antimicrobial stewardship. We discuss the implications for healthcare workforce training, managerial accountability under the NIS2 Directive, and the regulation of telemedicine platforms.

Key words: cybersecurity; telemedicine; ransomware; patient safety; NIS2 Directive; healthcare education.

Correspondence to: Paolo Sossai, Director, Department of Health, Maxi-Emergencies and Disaster International School (MEDIS), Modena; President, Central Medical Commission, Italian Alpine Club (CAI), Milan, Italy.
E-mail: info@paolosossai.eu

Introduction

In recent years, numerous hospitals in Italy and abroad have experienced cyberattacks that have temporarily disrupted electronic health records, laboratory systems, connected medical devices, and teleconsultation platforms. These incidents are no longer exceptional but recurrent, affecting healthcare facilities of all sizes across all countries. Telemedicine, which became a standard tool following the COVID-19 pandemic, has amplified this phenomenon: each connected device represents a potential access vector, and each teleconsultation platform a channel leading into clinical information systems.

The paradox is evident: the clinical effectiveness of digital medicine increases in proportion to its connectivity and, with it, its vulnerability also grows. Remote monitoring of cardiac patients, teleradiology that extends specialist expertise to peripheral areas, and teleconsultation that avoids the transport of critically ill patients all depend on networks, protocols, and access credentials that can be compromised.

Recent evidence

The healthcare sector is systematically among the most affected by cyberattacks. According to the Verizon Data Breach Investigations Report 2025,[1] which analyzed over 22,000 incidents and 12,195 confirmed breaches, the healthcare sector recorded 1,710 incidents, of which 1,542 involved confirmed data breaches, with system intrusion among the predominant attack patterns. Globally, third-party involvement - including supply chain and partners - has doubled, rising to 30% of breaches. The IBM Cost of a Data Breach Report 2025[2] documents that the average cost of a healthcare data breach reached USD 7.42 million in 2025 - the highest among the sectors analyzed for the fourteenth consecutive year - with an average time to identify and contain an incident of 279 days, also the highest among all sectors analyzed.

In Italy, the report by the National Cybersecurity Agency, "La minaccia cibernetica al settore sanitario", updated to September 2025,[3] documented an approximately 40% increase in cyber events affecting healthcare organizations in the first nine months of 2025 compared with the same period in 2024 (60 events *vs.* 42), continuing a growth trend that, over the 2023-2024 biennium, had reached 111%. The report highlights in particular the relevance of ransomware attacks, credential compromise, and malware dissemination via e-mail, within a context characterized by a widespread lack of basic security measures and insufficient targeted staff training.

More relevant from a clinical perspective are data linking cyberattacks to patient outcomes. The study by Neprash, McGlave, and Nikpay,[4] published in 2026 in the American Economic Journal, Economic Policy, analyzed Medicare data from 163 U.S. hospitals affected by ransomware attacks between 2016 and 2021,[5] using a Difference-in-Differences (DiD) design. The authors estimated that, among patients already hospitalized at the time of the attack, in-hospital mortality increased by 34-38%, while hospital activity volume declined by 17-24% during the week of the attack, with recovery

occurring within approximately three weeks. These are econometric estimates based on a model rather than individually verified causal links; however, the population-level signal is robust and replicable.

The fourth annual Cyber Insecurity in Healthcare report by the Ponemon Institute and Proofpoint, published in October 2025,[6] reports that 72% of healthcare organizations affected by major types of attacks (ransomware, cloud compromise, supply chain attacks, business email compromise) experienced interruptions in patient care, and that 29% of these reported an increase in mortality. The same study attributes a significant proportion of incidents to human factors - negligence, unintentional errors, lack of awareness, and non-compliance with organizational policies.

European and Italian Regulatory Framework

Directive (EU) 2022/2555 (NIS2), transposed in Italy by the Legislative Decree of September 4, 2024, No. 138,[7] has included the healthcare sector among those considered highly critical, imposing specific obligations for cyber risk management, 24-hour early notification, and full incident reporting within 72 hours of becoming aware of the incident, and assigning direct responsibility in this area to management and administrative bodies, which cannot be delegated solely to IT functions.

On the product side, Regulation (EU) 2017/745 on Medical Devices (MDR)[8] governs software with medical functions, while Regulation (EU) 2024/2847, known as the Cyber Resilience Act,[9] introduces horizontal cybersecurity requirements for products with digital elements. Medical devices regulated under the MDR are, however, excluded from the scope of the Cyber Resilience Act (Article 2) in order to avoid regulatory duplication: their cybersecurity remains governed by the MDR framework. The Cyber Resilience Act applies in full from December 11, 2027, but its Article 14, which requires manufacturers to report actively exploited vulnerabilities and severe incidents within 24 and 72 hours through the single reporting platform operated by ENISA, applies from September 11, 2026. Nevertheless, the boundary between the two regimes requires careful attention from manufacturers and user organizations across the entire supply chain. It should be noted that in December 2025 the European Commission proposed a revision of the MDR and the *In Vitro* Diagnostic Medical Devices (IVDR), which would remove the exemption of medical devices from the Cyber Resilience Act and integrate cybersecurity incident reporting into the MDR framework,[10] indicating that the boundary between the two regimes is evolving. However, a critical issue remains in the transition between certified devices and the network infrastructure through which their data are transmitted: a clinically validated device may still be exposed to cybersecurity risks if the operational environment does not ensure adequate security conditions.

A specific feature of telemedicine

Teleconsultation platforms, remote monitoring devices, and connected digital health applications now represent a rapidly expanding ecosystem, within a regulatory framework that is still in the process of consolidation. Without claiming exhaustiveness, we consider it useful to propose three operational principles that should guide the design and management of these solutions: i) minimum exposure - each connected device should transmit only the clinically necessary data, through encrypted channels and to authenticated recipients; ii) resilience by design - each platform should include business continuity procedures in the event of compromise, so as not to interrupt the delivery of care; iii) transparent accountability - developers and operators of telemedicine platforms should be publicly accountable for their security standards, with the same level of transparency applied to clinical effectiveness.

Cybersecurity as a clinical competency

The technical countermeasures currently recommended - network segmentation, multi-factor authentication, isolated and regularly tested backups, and the principle of minimum exposure - share an often-implicit assumption: that those who adopt and use them understand their clinical rationale. A strong password shared via messaging applications becomes a weak password; multi-factor authentication bypassed by approving an alert received in the middle of the night no longer provides protection; a backup that has never been tested is a promise, not a safeguard.

We therefore argue that healthcare cybersecurity should be recognized, at the operational, managerial, and organizational levels, as a clinical competency, rather than a mere administrative compliance requirement or a regulatory burden to be delegated to the Chief Information Officer. It is so in the same sense as hand hygiene, radiation protection, antimicrobial stewardship, or transfusion safety management: domain-specific technical practices that safeguard patient safety and whose link to clinical outcomes is now well established.

From this recognition, at least two operational consequences follow. The first concerns training. Basic cyber competencies - recognizing phishing attempts, properly managing access credentials, distinguishing a trusted network from a compromised one, understanding the functions and limitations of multi-factor authentication, and knowing what to report and to whom in the early hours of an incident - should be taught, practiced, and assessed with the same rigor as other fundamental clinical procedures. The prevailing model of a final-assessment e-learning module is inadequate for this purpose.

The second consequence concerns the governance level. The structure of the NIS2 Directive -which assigns explicit cybersecurity responsibilities to management and administrative bodies - is consistent with framing cyber posture as a dimension of clinical governance. A healthcare executive who does not understand, at least at a fundamental level, their attack surface and notification obligations would be in a position analogous to that of someone unfamiliar with their clinical outcome indicators.

Conclusions

The currently available evidence consistently indicates that cyberattacks targeting the healthcare sector do not produce only economic or reputational harm: they result in interruptions of care delivery, delays in clinical procedures and, in certain circumstances, excess mortality estimated at the population level. The European regulatory framework (NIS2, MDR, Cyber Resilience Act) provides a coherent normative structure; however, its effectiveness depends on the ability of healthcare systems to internalize cybersecurity as a clinical dimension, rather than as an additional compliance requirement.

From this perspective, investing in cybersecurity awareness and training for healthcare professionals does not constitute an ancillary cost: it is, in substance, a component of clinical education and a patient safety measure. What is at stake is not data protection: it is patient protection.

References

1. Verizon Communications Inc. 2025 Data Breach Investigations Report. Verizon Communications Inc.; Basking Ridge, USA; 2025.
2. IBM Corp. Security. Cost of a Data Breach Report 2025. IBM Corp.; Armonk, USA; 2025.
3. Agenzia Italiana per la Cybersicurezza Nazionale (ACN). La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni. Edizione aggiornata, periodo gennaio 2023 - settembre 2025. ACN; Rome, Italy; 2025.
4. Neprash HT, McGlave CC, Nikpay SS. Hacked to pieces? The effects of ransomware attacks on hospitals and patients. Am Econ J Econ Policy 2026;18:256-81.
5. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum 2022;3:e224873.
6. Ponemon Institute, Proofpoint. Cyber insecurity in healthcare: the cost and impact on patient safety and care 2025. Proofpoint; Sunnyvale, USA; 2025.
7. Decreto Legislativo 4 settembre 2024, n. 138. Attuazione della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2). Gazzetta Ufficiale della Repubblica Italiana n. 230, 1º ottobre 2024.
8. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices. Official Journal of the European Union, L 117, 5 May 2017.
9. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, L, 20 November 2024.
10. European Commission. Proposal for a revision of Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017/746 (IVDR). COM(2025) 1023 final. Strasbourg: European Commission; 16 December 2025.

Received: 1 September 2026; Accepted: 1 September 2026.

Contributions: both authors contributed to the conceptualization and design of the work, the literature review, the drafting, and the critical revision of the manuscript. Both authors have read and approved the final version of the manuscript, and agreed to be held accountable for all aspects of the work.

Conflict of interest: the authors declare the following potentially relevant relationships in relation to the topics addressed. Since 2022, Prof. Paolo Sossai has been under an ongoing annual contract with Alchimie Digitali S.r.l. for the maintenance of his professional website. Nicola Fabbri is Director of Sales, Marketing & Business Development at Alchimie Digitali S.r.l., a company operating commercially in the fields of Data Protection, Cybersecurity, and GDPR/NIS2 Compliance. This editorial does not discuss, recommend, or evaluate any specific products or services of Alchimie Digitali S.r.l. No funding was received for the preparation of this manuscript, and the authors received no remuneration for its preparation. Given that Paolo Sossai is Editor-in-Chief of Telemedicine International, he did not participate in any editorial decision concerning this manuscript, which was handled independently by the journal's editorial office. As an Editorial, this article underwent editorial review by the editorial office and was not submitted to external peer review, in accordance with the journal's policy for opinion content. The authors further declare that they have no other financial, advisory, or intellectual property relationships relevant to the content of this article.

Funding: none.

Ethics approval and consent to participate: not applicable.

Informed consent: not applicable.

Availability of data and materials: all data generated or analyzed during this study are included in this published article.