MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Public Health Open Access
ISSN: 2578-5001

Cybersecurity in Healthcare: Why It Must Be Recognized as a Public Health Priority

Rao R*

Department of Healthcare, Western Sydney University, Australia

***Corresponding author:** Radhika Rao, Department of Healthcare, Western Sydney University, Australia

Commentary

Volume 10 Issue 1

Received Date: June 01, 2026

Published Date: June 25, 2026

Abstract

The rapid digitalization of healthcare has transformed patient care, disease surveillance, and health system management. However, this transformation has also exposed healthcare systems to increasing cybersecurity risks that threaten not only data privacy but also patient safety and public health. Cyberattacks on healthcare institutions can interrupt essential medical services, compromise disease surveillance, delay emergency responses, and undermine public confidence in health systems. This commentary argues that cybersecurity should no longer be viewed solely as a technical or information technology concern but as a critical component of public health preparedness and healthcare resilience. Strengthening cybersecurity through effective governance, workforce education, and investment in secure digital infrastructure is essential for protecting population health in the digital era.

Keywords: Cybersecurity; Public Health; Digital Health; Patient Safety; Health Information Systems; Healthcare Resilience

Commentary

Healthcare is experiencing one of the most significant technological transformations in its history. Electronic health records, telemedicine, artificial intelligence, wearable technologies, cloud computing, and mobile health applications have become integral to healthcare delivery. These innovations have improved communication, expanded access to healthcare, and enhanced clinical decision-making. Nevertheless, they have also introduced new vulnerabilities that extend far beyond the information technology department.

Cybersecurity is often discussed as a technical issue, but its implications are much broader. A cyberattack on a healthcare organization can disrupt emergency care, delay surgeries, interrupt laboratory services, and restrict access to life-saving patient information. Such consequences directly affect patient outcomes and, consequently, public health. For this reason, cybersecurity deserves recognition as a public health priority rather than simply an operational concern [1].

Recent cyber incidents affecting healthcare institutions worldwide have demonstrated how dependent modern healthcare has become on digital infrastructure. Even brief disruptions in hospital information systems may delay diagnosis and treatment, particularly for critically ill patients. Public health agencies also rely on secure digital platforms for disease surveillance, vaccination programs, laboratory reporting, and emergency preparedness. If these systems are compromised, the ability to detect outbreaks or coordinate public health responses may be significantly weakened [2].

CC BY

The COVID-19 pandemic accelerated digital health adoption across the world. Telemedicine became essential for maintaining continuity of care, while electronic reporting systems supported surveillance and public health decision-making. Although these technologies improved healthcare accessibility, they also expanded the attack surface available to cybercriminals. The increasing reliance on interconnected digital systems makes cybersecurity an indispensable component of healthcare resilience.

In my view, one of the greatest misconceptions is that cybersecurity concerns only patient privacy. Protecting confidential information is undoubtedly important, but cybersecurity also protects healthcare delivery itself. Clinical decision-making increasingly depends on immediate access to accurate electronic health records. Medical devices, diagnostic equipment, and communication systems are interconnected, meaning that disruptions can affect the entire continuum of patient care [3].

Healthcare organizations should therefore integrate cybersecurity into patient safety initiatives. Just as hospitals routinely prepare for infectious disease outbreaks, natural disasters, and mass casualty incidents, they should also develop comprehensive cybersecurity preparedness plans. Regular risk assessments, incident response exercises, secure data backup strategies, and continuous system monitoring should become routine components of healthcare management.

Another important consideration is the human element. Technology alone cannot prevent every cyber incident. Healthcare professionals remain the first line of defense against phishing emails, unauthorized access, and accidental disclosure of confidential information. Continuous education and practical cybersecurity training should become part of routine professional development for all healthcare personnel, regardless of their clinical role.

Policy makers also have an important responsibility. National digital health strategies should incorporate cybersecurity standards from the earliest stages of implementation. Investment in healthcare digitalization must be accompanied by proportional investment in cybersecurity infrastructure, workforce capacity, and regulatory oversight. Failure to balance innovation with security may expose healthcare systems to unnecessary risks.

Health equity should also be considered when discussing cybersecurity. Many healthcare facilities in low- and middle-income countries continue to face financial and technical barriers that limit implementation of robust cybersecurity measures. These institutions often experience growing digitalization without corresponding investment in security infrastructure. International collaboration and technical support will therefore be necessary to reduce disparities and strengthen global health security.

Artificial intelligence presents both opportunities and challenges. AI-based systems can rapidly identify abnormal network activity and detect potential cyber threats before significant damage occurs. At the same time, artificial intelligence itself requires transparent governance and ongoing evaluation to ensure that automated decisions remain reliable, ethical, and secure. Human oversight will continue to play an essential role in cybersecurity decision-making.

Cybersecurity should no longer be viewed as an isolated responsibility of information technology professionals. It requires collaboration among clinicians, hospital administrators, public health experts, engineers, policymakers, and cybersecurity specialists. Such multidisciplinary cooperation strengthens healthcare resilience while protecting both individual patients and entire populations.

As healthcare continues to evolve, digital trust will become increasingly important. Patients are more willing to engage with electronic health records, telemedicine services, and mobile health applications when they have confidence that their information remains secure. Maintaining this trust is essential for successful digital health implementation and long-term public health improvement.

The future of healthcare depends on digital innovation, but innovation cannot succeed without security. Healthcare organizations should adopt cybersecurity-by-design principles when implementing new technologies and continuously evaluate emerging risks as digital systems expand. Public health preparedness in the twenty-first century must include preparedness for cyber threats alongside biological and environmental hazards.

Conclusion

Cybersecurity has become an essential determinant of healthcare system resilience and should be recognized as a public health priority. Protecting healthcare information systems safeguards not only patient privacy but also the continuity of healthcare services, disease surveillance, emergency response, and public confidence in health systems. Governments, healthcare organizations, technology developers, and public health professionals must work collaboratively to strengthen cybersecurity policies, improve workforce education, and invest in secure digital

Copyright© Rao R.

infrastructure. By embedding cybersecurity into public health planning, healthcare systems will be better prepared to respond to both current and future challenges in an increasingly digital world.

Conflict of Interest

The author declares no conflict of interest.

Funding

The author received no financial support for the preparation of this commentary.

References

1. World Health Organization (2024) Addressing Future Cybersecurity Threats in Digital Health: Report of the Technical Consultation, Geneva, Switzerland.

2. Marron J (2024) Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide.

3. World Health Organization (2025) Regional Office for Europe. Cybersecurity and Privacy Maturity Assessment and Strengthening for Digital Health Information Systems.

Copyright© Rao R.