From Data To Protection: The Role Of Nursing And Computerized Medical Records In Preventive Healthcare And Health Security

Nura Saad Almutairi[1], Abdulrahman Fahd Mansour Al-Dabaa[2], Nadiyah Karim Alenezi[3], Alaa Hamad Alyami[4], Nizar Saleh Alshabaan[5], Faisal Mousa Ayesh Al-Rashidi[6], Raya h Saud Menwer Almutairi[7], Mohammed Ayidh Hamad Al Aqil[8], Abdulilah Ibrahim Mohammed Althuwayb[9], Bader Abdulaziz Fahad Alrusaini[10]

[1]Nursing – Health Cluster 2 – Riyadh, Saudi Arabia
[2] Nursing – Buraidah Central Hospital – Buraidah, Saudi Arabia
[3]Preventive Medicine Consultant – Ministry of Health – Al Madinah, Saudi Arabia
[4]Preventive Medicine Consultant – Ministry of Health – Tabuk, Saudi Arabia
[5]Medical Records Technician – Qassim Armed Forces Hospital – Al Qassim, Saudi Arabia
[6]Health Security – King Fahad Specialist Hospital – Buraidah, Saudi Arabia
[7]Health Security – Al-Faiha Primary Healthcare Center – Al Majmaah, Saudi Arabia
[8]Nursing Specialist – New Najran General Hospital – Najran, Saudi Arabia
[9]Health Informatics Technician – Armed Forces Hospital in Qassim – Al-Rass, Saudi Arabia
[10]Health Assistant – Armed Forces Hospital in Qassim – Onaizah, Saudi Arabia

Abstract

The rapid digitalization of healthcare systems has positioned computerized medical records (CMRs) as a cornerstone for strengthening preventive healthcare and advancing health security. This narrative and conceptual review examines the role of nursing in leveraging CMRs to transform health data into proactive protection at both individual and system levels. Drawing on interdisciplinary literature, the review explores how nursing practice, preventive healthcare strategies, and digital health infrastructures intersect to enhance surveillance, early risk detection, continuity of care, and preparedness for health threats.

The analysis demonstrates that while CMRs significantly support preventive healthcare and health security, their effectiveness depends on multiple interconnected factors. These include technical infrastructure and interoperability, nursing digital competencies, organizational culture, leadership commitment, and robust data governance frameworks. Nurses play a pivotal role as primary users and producers of health data, contributing to accurate documentation, patient education, infection prevention, and early warning mechanisms that underpin health security efforts.

Ethical considerations—particularly data privacy, confidentiality, and professional accountability—emerge as critical determinants of trust and system resilience. The review emphasizes that health security should be embedded within everyday nursing practice and preventive care rather than viewed solely as an emergency response function. Overall, the findings highlight that moving "from data to protection" requires a holistic, multidisciplinary approach in which nursing leadership, digital health systems, and preventive strategies are aligned to support sustainable and secure healthcare systems.

This review is informed by authoritative and peer-reviewed sources, including reports and frameworks from the World Health Organization (WHO), the Organisation for Economic Co-operation and Development (OECD), and leading journals in digital health, nursing, and public health.

Keywords: Nursing; computerized medical records; preventive healthcare; health security; digital health; healthcare systems.

INTRODUCTION

Over the past two decades, healthcare systems worldwide have undergone a profound digital transformation driven by the expansion of computerized medical records (CMRs), also referred to as electronic medical records (EMRs) or electronic health records (EHRs). These systems have evolved from basic documentation tools into complex infrastructures that support clinical decision-making, population health surveillance, preventive care strategies, and health security preparedness (WHO, 2022; Adler-Milstein & Huckman, 2013).

Computerized medical records play a central role in organizing, storing, and exchanging health information across multiple levels of care. Beyond improving clinical efficiency, CMRs contribute to early disease detection, monitoring of public health threats, and coordination of preventive interventions (Bates et al., 2014; Menachemi & Collum, 2011). Their importance became particularly evident during global health emergencies, where timely access to accurate data was essential for outbreak surveillance, risk communication, and resource allocation (Keesara et al., 2020; WHO, 2021).

Preventive healthcare relies heavily on high-quality data to identify risk factors, monitor trends, and implement evidence-based interventions. Digital health records enable longitudinal tracking of patient health, facilitate screening programs, and support population-level preventive strategies (Gagnon et al., 2016; Kruse et al., 2018). When effectively implemented, CMRs enhance continuity of care and strengthen preventive health outcomes.

Health security, defined as the capacity of health systems to prevent, detect, and respond to health threats, has emerged as a global priority in the context of pandemics, bioterrorism risks, and cyber threats to health data (Katz et al., 2018; WHO, 2019). In this framework, computerized medical records serve as a critical link between individual-level care and system-wide protection. However, the success of this integration does not depend on technology alone; it is shaped by organizational readiness, workforce competencies, governance structures, ethical safeguards, and interprofessional collaboration (Cresswell et al., 2020; Shaw et al., 2018).

This article adopts a narrative and conceptual approach to examine how computerized medical records contribute to preventive healthcare and health security. It explores the multifactorial conditions under which digital health systems successfully move “from data to protection,” emphasizing the roles of nursing, preventive medicine, medical records professionals, and health security practitioners.

2. CONCEPTUAL FRAMEWORK

2.1 Computerized Medical Records

Computerized medical records are digital systems designed to capture, store, and manage patient health information across clinical and administrative domains. They encompass medical histories, diagnostic results, treatment plans, and preventive care data, enabling real-time access and interoperability among healthcare providers (ISO, 2019; HIMSS, 2020).

The conceptual value of CMRs extends beyond data storage. They function as foundational components of health information systems that support clinical governance, quality assurance, and health surveillance (Boonstra et al., 2014). Studies have shown that wellimplemented CMRs improve clinical outcomes, reduce medical errors, and enhance coordination of care (Bates et al., 2014; Kruse et al., 2016).

From a health security perspective, computerized records enable early warning systems, syndromic surveillance, and rapid reporting of notifiable diseases (CDC, 2020; Yasnoff et al., 2000). They also play a vital role in safeguarding sensitive health data, raising critical considerations related to cybersecurity, data integrity, and patient privacy (Rindfleisch, 2017; OECD, 2020).

2.2 Preventive Healthcare

Preventive healthcare focuses on reducing disease burden through proactive measures, including health promotion, screening, early diagnosis, and risk mitigation. It is commonly categorized into primary, secondary, and tertiary prevention, all of which increasingly depend on digital data infrastructures (Gulliford, 2012; WHO, 2018).

Computerized medical records support preventive healthcare by enabling population health analytics, identifying high-risk groups, and facilitating evidence-based interventions (Glasgow et al., 2012; Goldstein et al., 2017). The integration of CMRs into preventive strategies enhances continuity of care and allows healthcare professionals to shift from reactive treatment to anticipatory health management.

Furthermore, preventive healthcare contributes directly to health security by reducing vulnerability to outbreaks, managing chronic disease burdens, and strengthening system resilience (Kickbusch et al., 2016; Frenk et al., 2014). Digital records provide the informational backbone necessary for coordinated preventive responses at institutional and national levels.

2.3 Health Security

Health security encompasses policies, systems, and practices aimed at protecting populations from health threats, including infectious diseases, environmental hazards, and system disruptions (WHO, 2019). It integrates clinical care, public health, emergency preparedness, and information governance.

In the digital era, health security is inseparable from data security. Computerized medical records contribute to situational awareness, crisis response, and cross-sector coordination but also introduce risks related to cyberattacks and data breaches (Kostkova et al., 2016; Kruse et al., 2017). Effective health security therefore depends on aligning technological capacity with ethical frameworks, legal protections, and professional accountability.

3. Interrelationship Between Computerized Medical Records, Preventive Healthcare, and Health Security

The relationship between computerized medical records (CMRs), preventive healthcare, and health security is inherently synergistic. Rather than functioning as isolated components, these elements collectively form an integrated system that enables healthcare organizations to move from reactive care toward proactive protection (Kostkova et al., 2016; WHO, 2022).

Computerized medical records provide the informational infrastructure necessary for effective preventive healthcare. Through longitudinal data collection and real-time accessibility, CMRs allow healthcare professionals to identify emerging health risks, monitor disease patterns, and implement timely preventive interventions (Yasnoff et al., 2000; Glasgow et al., 2012). Screening programs, immunization tracking, and chronic disease management increasingly rely on digital records to ensure continuity and accuracy of preventive efforts (Goldstein et al., 2017; Kruse et al., 2018).

From a health security perspective, preventive healthcare represents the first line of defense against systemic threats. By reducing disease incidence and improving early detection, prevention directly enhances the resilience of health systems (Kickbusch et al., 2016; Frenk et al., 2014). Computerized medical records strengthen this function by enabling syndromic surveillance, outbreak detection, and rapid reporting to public health authorities (CDC, 2020; ECDC, 2018).

Health security further depends on the capacity of systems to integrate clinical data with public health intelligence. CMRs facilitate this integration by supporting interoperability between healthcare facilities, laboratories, and public health agencies (HIMSS, 2020; ISO, 2019). During public health emergencies, such integration allows for coordinated responses, resource optimization, and evidence-based decision-making (Keesara et al., 2020; Shaw et al., 2018).

However, the effectiveness of this interrelationship is shaped by multiple contextual factors. Organizational culture, workforce readiness, governance frameworks, and ethical safeguards influence how data are collected, interpreted, and utilized (Cresswell et al., 2020; Greenhalgh et al., 2017). Inadequate data quality, fragmented systems, or weak security measures can undermine both preventive outcomes and health security objectives (Rindfleisch, 2017; OECD, 2020).

Thus, the transition "from data to protection" reflects a multidimensional process in which computerized medical records serve as enablers rather than guarantees of success. Preventive healthcare and health security outcomes emerge when digital systems are aligned with professional practice, institutional accountability, and regulatory oversight (WHO, 2019; Katz et al., 2018).

4. Multidisciplinary Roles in Advancing Health Security

Health security in the digital era is not achieved through technology alone but through coordinated multidisciplinary practice. Computerized medical records (CMRs) act as a shared platform that enables collaboration among nursing professionals, preventive medicine specialists, medical records practitioners, and health security personnel. Each discipline contributes distinct competencies that collectively transform health data into protective action (WHO, 2019; Frenk et al., 2014).

4.1 Nursing

Nursing professionals are primary users and generators of clinical data within computerized medical records. Accurate and timely nursing documentation is essential for continuity of care, early detection of patient deterioration, and implementation of preventive interventions (Ammenwerth & Keizer, 2007; Wang et al., 2018). Through routine assessments, nurses contribute critical real-time data that support infection prevention, medication safety, and patient risk stratification.

From a health security perspective, nursing documentation within CMRs enhances surveillance capabilities and supports early warning systems for adverse events and infectious outbreaks (Stone et al., 2018; WHO, 2021). Nurses also play a key role in patient education and adherence to preventive measures, thereby reinforcing system-wide resilience and preparedness.

4.2 Preventive Medicine

Preventive medicine specialists utilize computerized medical records to analyze population-level data, identify emerging health risks, and design evidence-based preventive strategies. CMRs facilitate screening programs, vaccination monitoring, and chronic disease prevention through integrated data analytics (Glasgow et al., 2012; Gulis & Fujino, 2015).

In the context of health security, preventive medicine bridges clinical care and public health surveillance. Digital records enable timely reporting of notifiable diseases, support epidemiological investigations, and inform policy responses during health emergencies (CDC, 2020; ECDC, 2018). This data-driven approach strengthens early detection and rapid response mechanisms that are central to health security frameworks.

4.3 Medical Records and Health Information Professionals

Medical records professionals ensure the quality, accuracy, standardization, and confidentiality of health data within computerized systems. Their role is fundamental to maintaining data integrity, interoperability, and compliance with legal and ethical standards (AHIMA, 2020; ISO, 2019).

High-quality data governance directly influences health security outcomes. Inaccurate or incomplete records can compromise surveillance, misinform preventive strategies, and weaken emergency responses (OECD, 2020; Kruse et al., 2017). Health information professionals therefore act as custodians of digital trust, safeguarding patient privacy while enabling legitimate data use for protection and preparedness.

4.4 Health Security Professionals

Health security professionals focus on risk assessment, emergency preparedness, and protection of health systems from biological, environmental, and digital threats. Computerized medical records provide essential situational awareness by integrating clinical data with public health intelligence and emergency management systems (Katz et al., 2018; WHO, 2019).

In addition, the increasing reliance on digital health records introduces cybersecurity risks that fall within the scope of health security. Collaboration between health security experts and information governance teams is critical to protecting sensitive health data from cyberattacks and system failures (Rindfleisch, 2017; Kostkova et al., 2016). Effective health security thus depends on aligning technological safeguards with professional accountability and institutional governance.

5. Factors Influencing the Success of Computerized Medical Records in Preventive Healthcare and Health Security

The effectiveness of computerized medical records (CMRs) in strengthening preventive healthcare and health security is contingent upon a complex interaction of technical, human, organizational, and ethical factors. Evidence consistently shows that digital health technologies alone do not guarantee improved outcomes; rather, success emerges when systems are embedded within supportive institutional and professional environments (Greenhalgh et al., 2017; Cresswell et al., 2020).

5.1 Technical and Infrastructure Factors

Robust digital infrastructure is a prerequisite for the effective use of CMRs. System reliability, interoperability, data standardization, and cybersecurity capacity directly affect the usability and trustworthiness of health records (ISO, 2019; HIMSS, 2020). Fragmented systems and poor interoperability hinder data sharing between healthcare providers and public health authorities, undermining preventive surveillance and coordinated responses to health threats (Adler-Milstein et al., 2017; WHO, 2022).

Cybersecurity has become a critical technical concern for health security. Increasing cyberattacks on healthcare systems threaten data integrity, service continuity, and public trust (Kruse et al., 2017; Rindfleisch, 2017). Secure system design and continuous monitoring are therefore essential components of health protection in digital environments.

5.2 Human and Workforce Factors

Healthcare professionals' digital competencies strongly influence the success of computerized medical records. Training, digital literacy, and user engagement determine how effectively CMRs are integrated into clinical and preventive workflows (Gagnon et al., 2016; Ammenwerth et al., 2019). Resistance to change, increased documentation burden, or poor system usability can reduce adoption and compromise data quality (Boonstra et al., 2014; Kruse et al., 2016).

From a health security perspective, workforce readiness extends beyond technical skills to include awareness of data protection, ethical responsibilities, and emergency protocols. Interprofessional collaboration among nurses, preventive medicine specialists, health information professionals, and health security personnel is essential for translating data into coordinated protective action (Frenk et al., 2014; WHO, 2019).

5.3 Organizational and Governance Factors

Strong governance structures play a decisive role in aligning CMRs with preventive and security objectives. Clear policies on data use, accountability, and system oversight support consistent implementation and reduce variability across institutions (OECD, 2020; Shaw et al., 2018). Leadership commitment and organizational culture influence whether digital systems are used strategically or merely as administrative tools (Cresswell et al., 2020).

Inadequate governance can result in fragmented data practices, weak surveillance capacity, and delayed responses during public health emergencies (Katz et al., 2018; WHO, 2021). Conversely, organizations that integrate digital health governance into broader health security frameworks demonstrate greater resilience and preparedness.

5.4 Ethical and Legal Factors

Ethical and legal considerations are central to the success of computerized medical records. Patient privacy, informed consent, and data ownership shape public trust in digital health systems (OECD, 2020; Mittelstadt, 2017). Breaches of confidentiality or misuse of data can undermine both preventive healthcare initiatives and health security efforts.

Balancing data accessibility for surveillance and prevention with respect for individual rights represents an ongoing challenge (Floridi et al., 2018; WHO, 2019). Effective legal frameworks and ethical guidelines are therefore essential to ensure that the use of CMRs enhances protection without compromising fundamental values.

6. Challenges and Ethical Considerations

Despite the recognized potential of computerized medical records (CMRs) to enhance preventive healthcare and health security, multiple challenges and ethical concerns continue to limit their effectiveness. These challenges span technological vulnerabilities, organizational constraints, and ethical dilemmas related to data use and protection (Cresswell et al., 2020; WHO, 2019).

6.1 Cybersecurity Threats and System Vulnerabilities

The increasing digitization of health records has expanded the attack surface for cyber threats targeting healthcare systems. Ransomware attacks, data breaches, and system disruptions pose significant risks to patient safety, service continuity, and public trust (Kruse et al., 2017; Gordon & Fairhall, 2021). From a health security standpoint, compromised digital systems can undermine surveillance, delay emergency responses, and disrupt preventive services during critical periods.

Healthcare organizations often face constraints related to outdated infrastructure, limited cybersecurity expertise, and insufficient investment in digital protection (Rindfleisch, 2017; OECD, 2020). These vulnerabilities highlight the need to integrate cybersecurity as a core component of health security planning rather than treating it as a purely technical issue.

6.2 Digital Inequities and the Implementation Gap

Digital transformation has not progressed uniformly across healthcare systems. Variations in resources, infrastructure, and workforce capacity contribute to a digital divide between and within countries (WHO, 2021; van Dijk, 2020). Such disparities can limit the reach of preventive healthcare initiatives and weaken system-wide health security.

Inconsistent adoption of CMRs results in fragmented data, reduced interoperability, and uneven surveillance coverage. This implementation gap can compromise early detection of health threats and reduce the effectiveness of coordinated preventive responses (Greenhalgh et al., 2017; Adler-Milstein et al., 2017).

6.3 Privacy, Confidentiality, and Data Governance

Ethical concerns related to privacy and confidentiality remain central to the use of computerized medical records. Health data are highly sensitive, and unauthorized access or misuse can cause harm to individuals and erode confidence in digital health systems (Mittelstadt, 2017; Floridi et al., 2018).

Balancing the need for data accessibility to support prevention and surveillance with respect for individual rights presents an ongoing ethical challenge. Health security initiatives often require rapid data sharing across institutions and jurisdictions, raising questions about consent, proportionality, and transparency (OECD, 2020; WHO, 2019). Robust data governance frameworks are therefore essential to ensure ethical and lawful data use.

6.4 Professional Accountability and Ethical Practice

The effective use of computerized medical records also depends on professional accountability. Inaccurate documentation, inappropriate data access, or lack of adherence to ethical guidelines can undermine both preventive healthcare and health security objectives (AHIMA, 2020; Ammenwerth et al., 2019).

Ethical practice requires continuous training, clear role delineation, and institutional support for responsible data use. Interdisciplinary collaboration is particularly important in managing ethical tensions between data protection and public health imperatives during emergencies (Frenk et al., 2014; WHO, 2021).

7. Implications for Healthcare Culture

The integration of computerized medical records (CMRs) into preventive healthcare and health security frameworks has profound implications for healthcare culture. Digital transformation reshapes not only clinical workflows but also professional values, communication patterns, and institutional priorities, influencing how healthcare organizations perceive prevention, responsibility, and protection (Greenhalgh et al., 2017; WHO, 2022).

7.1 From Reactive Care to a Culture of Prevention

Traditionally, many healthcare systems have emphasized reactive, treatment-oriented models of care. The widespread adoption of CMRs supports a cultural shift toward prevention by enabling early risk identification, continuous monitoring, and data-driven decision-making (Glasgow et al., 2012; Goldstein et al., 2017). When preventive insights are embedded in daily practice through digital records, prevention becomes a shared organizational value rather than an isolated public health function.

This cultural transition reinforces health security by reducing system vulnerability to avoidable health threats and strengthening preparedness through anticipatory action (Kickbusch et al., 2016; Frenk et al., 2014).

7.2 Professional Collaboration and Shared Accountability

Computerized medical records foster interprofessional collaboration by creating a shared informational environment across disciplines. Nurses, preventive medicine specialists, medical records professionals, and health security practitioners access and contribute to the same data ecosystem, promoting transparency and shared accountability (Frenk et al., 2014; Cresswell et al., 2020).

Such collaboration reshapes healthcare culture from siloed professional practice to integrated teamwork. In this context, health security is understood as a collective responsibility that extends beyond emergency response to encompass everyday documentation practices, preventive interventions, and ethical data use (WHO, 2019; AHIMA, 2020).

7.3 Trust, Transparency, and Ethical Culture

Trust is a central cultural determinant of successful digital health implementation. Patients' willingness to engage with preventive programs and share health information depends on confidence in data protection, ethical governance, and professional integrity (Floridi et al., 2018; OECD, 2020). CMRs can strengthen trust when used transparently and responsibly, but they can also undermine it if associated with breaches or misuse.

An ethical healthcare culture emphasizes respect for privacy, informed consent, and proportional data use while recognizing the legitimate needs of public health and health security (Mittelstadt, 2017; WHO, 2019). Embedding these principles into organizational culture is essential for sustaining both preventive healthcare and system-wide protection.

7.4 Health Security as a Cultural Norm

Viewing health security as a cultural norm rather than a crisis-driven response represents a critical evolution in healthcare systems. Digital records contribute to this shift by normalizing surveillance, preparedness, and risk management as routine aspects of care delivery (Kostkova et al., 2016; Katz et al., 2018).

In this cultural framing, computerized medical records function as instruments of institutional memory and learning, enabling organizations to adapt, improve, and protect populations over time. Such a perspective aligns closely with the interdisciplinary and reflective ethos of contemporary healthcare culture.

8. Future Directions

The future of computerized medical records (CMRs) in preventive healthcare and health security lies in advancing from passive data repositories toward intelligent, integrated, and resilient digital ecosystems. Emerging technologies, evolving governance models, and strengthened workforce capabilities are expected to shape how health systems translate data into sustained protection (WHO, 2022; Topol, 2019).

8.1 Artificial Intelligence and Predictive Analytics

Artificial intelligence (AI) and advanced analytics are increasingly integrated into CMR platforms to enhance risk prediction, early detection, and decision support. Machine learning algorithms can analyze large-scale health data to identify patterns associated with disease outbreaks, chronic disease progression, and system vulnerabilities (Esteva et al., 2019; Rajkomar et al., 2019).

From a health security perspective, predictive analytics support anticipatory action by enabling early warnings and targeted preventive interventions. However, their effectiveness depends on data quality, transparency of algorithms, and ethical oversight to prevent bias and ensure accountability (Floridi et al., 2018; WHO, 2021).

8.2 Interoperability and Integrated Health Information Systems

Achieving seamless interoperability across healthcare, public health, and emergency management systems remains a strategic priority. Integrated CMRs enable coordinated surveillance, rapid information exchange, and unified responses to health threats at local, national, and global levels (HIMSS, 2020; Adler-Milstein et al., 2017).

Future health security frameworks are likely to emphasize standardized data architectures and cross-sector collaboration to reduce fragmentation and enhance situational awareness during crises (Katz et al., 2018; OECD, 2020).

8.3 Strengthening Digital Governance and Regulatory Frameworks

As digital health systems expand, robust governance mechanisms are essential to balance innovation with protection. Future directions include clearer regulatory standards for data sharing, cybersecurity, and ethical use of health information (OECD, 2020; WHO, 2019).

Embedding digital governance within broader health security strategies can enhance trust, legitimacy, and system resilience. Such alignment ensures that preventive healthcare initiatives and emergency preparedness efforts are supported by consistent legal and ethical foundations (Shaw et al., 2018; Mittelstadt, 2017).

8.4 Workforce Development and Digital Health Literacy

Sustainable progress in digital health security requires continuous investment in workforce development. Training programs that enhance digital health literacy, ethical awareness, and interprofessional collaboration are critical to maximizing the value of CMRs (Gagnon et al., 2016; Frenk et al., 2014).

Future-oriented education should prepare healthcare professionals to engage with evolving technologies while maintaining a patient-centered and security-conscious approach to care delivery (WHO, 2021; Ammenwerth et al., 2019).

9. CONCLUSION

The growing integration of computerized medical records into healthcare systems represents a critical shift from data collection toward proactive protection. As demonstrated throughout this narrative review, the contribution of digital health records to preventive healthcare and health security extends far beyond technological functionality. Their true value emerges when they are embedded within supportive organizational cultures, ethical governance frameworks, and multidisciplinary professional practice (WHO, 2019; Greenhalgh et al., 2017).

Computerized medical records enable continuity of care, support preventive strategies, and enhance surveillance and preparedness capacities that are essential for health security. However, success is not determined by digitalization alone. Technical infrastructure, workforce competencies, leadership commitment, ethical safeguards, and interprofessional collaboration collectively shape the effectiveness of these systems in translating data into protection (Cresswell et al., 2020; OECD, 2020).

The findings highlight that nursing, preventive medicine, medical records professionals, and health security practitioners play complementary roles in strengthening health system resilience. Their coordinated engagement transforms computerized records into instruments of prevention, trust, and preparedness rather than mere repositories of information (Frenk et al., 2014; Katz et al., 2018).

From a cultural perspective, embracing health security as an integral and routine component of healthcare practice represents a necessary evolution. Digital records can foster this cultural shift by normalizing prevention, accountability, and ethical data use within everyday clinical and organizational workflows (Kickbusch et al., 2016; WHO, 2022).

In conclusion, moving "from data to protection" requires a holistic approach that aligns technology with human values, governance, and professional responsibility. Such an approach is essential for ensuring that computerized medical records effectively support preventive healthcare and contribute meaningfully to sustainable health security in an increasingly complex digital era.

References

1. Adler-Milstein, J., & Huckman, R. S. (2013). The impact of electronic health record use on physician productivity. *American Journal of Managed Care, 19*(10), 345–352.

2. Adler-Milstein, J., Pfeifer, E., & Searcy, T. (2017). Interoperability of electronic health records and health information exchange. *Health Affairs, 36*(7), 1226–1233. https://doi.org/10.1377/hlthaff.2016.1466

3. Ammenwerth, E., & Keizer, N. (2007). Nursing documentation systems: A review of the literature. *Journal of the American Medical Informatics Association, 14*(6), 747–757. https://doi.org/10.1197/jamia.M240

4. Ammenwerth, E., Iller, C., & Mahler, C. (2019). IT-adoption and the interaction of task, technology and individuals. *Methods of Information in Medicine, 58*(1), 1–8. https://doi.org/10.1055/s-0039-1687839

5. Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. (2014). Big data in health care: Using analytics to identify and manage high-risk patients. *Health Affairs, 33*(7), 1123–1131. https://doi.org/10.1377/hlthaff.2014.0041

6. Boonstra, A., Versluis, A., & Vos, J. F. J. (2014). Implementing electronic health records in hospitals: A systematic literature review. *BMC Health Services Research, 14*, 370. https://doi.org/10.1186/1472-6963-14-370

7. Centers for Disease Control and Prevention. (2020). *Public health surveillance and data systems*. CDC.

8. Cresswell, K., Sheikh, A., & Krasuska, M. (2020). Reconceptualising the digital health implementation challenge. *Journal of Medical Internet Research, 22*(9), e19259. https://doi.org/10.2196/19259

9. Esteva, A., Robicquet, A., Ramsundar, B., et al. (2019). A guide to deep learning in healthcare. *Nature Medicine, 25*(1), 24–29. https://doi.org/10.1038/s41591-018-0316-z

10. Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society. *Philosophical Transactions of the Royal Society A, 376*(2133), 20180002. https://doi.org/10.1098/rsta.2018.0002

11. Frenk, J., Chen, L., Bhutta, Z. A., et al. (2014). Health professionals for a new century. *The Lancet, 384*(9945), 2229–2254. https://doi.org/10.1016/S0140-6736(14)61651-2

12. Gagnon, M. P., Ghandour el, K., Talla, P. K., et al. (2016). Electronic health record adoption by physicians. *Implementation Science, 11*, 72. https://doi.org/10.1186/s13012-016-0437-9

13. Glasgow, R. E., Phillips, S. M., & Sanchez, M. A. (2012). Implementation science approaches for integrating eHealth research. *American Journal of Preventive Medicine, 42*(2), 127–135. https://doi.org/10.1016/j.amepre.2011.10.021

14. Goldstein, B. A., Navar, A. M., Pencina, M. J., & Ioannidis, J. P. A. (2017). Opportunities and challenges in developing risk prediction models. *Journal of the American Medical Informatics Association, 24*(6), 1119–1128. https://doi.org/10.1093/jamia/ocx042

15. Greenhalgh, T., Wherton, J., Papoutsi, C., et al. (2017). Beyond adoption: A new framework for theorizing and evaluating nonadoption of health technologies. *Journal of Medical Internet Research, 19*(11), e367. https://doi.org/10.2196/jmir.8775

16. HIMSS. (2020). *Interoperability in healthcare*. Healthcare Information and Management Systems Society.

17. International Organization for Standardization. (2019). *Health informatics—Information security management (ISO/IEC 27799)*. ISO.

18. Katz, R., Standley, C. J., Sorrell, E. M., et al. (2018). Global health security agenda and the international health regulations. *BMJ Global Health, 3*(2), e000545. https://doi.org/10.1136/bmjgh-2017-000545

19. Kickbusch, I., & Szabo, M. M. (2016). A new governance space for health. *The Lancet, 387*(10020), 2305–2306. https://doi.org/10.1016/S0140-6736(16)30276-1

20. Kostkova, P., Brewer, H., de Lusignan, S., et al. (2016). Who owns the data? *Philosophical Transactions of the Royal Society A, 374*(2069), 20160113. https://doi.org/10.1098/rsta.2016.0113

21. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *BMJ Health & Care Informatics, 24*(1), 1–8.

https://doi.org/10.14236/jhi.v24i1.963

22. Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy, 4*, 47–55. https://doi.org/10.2147/RMHP.S12985

23. Mittelstadt, B. (2017). Ethics of health data analytics. *Journal of Medical Ethics, 43*(12), 761–768. https://doi.org/10.1136/medethics-2016-103675

24. Organisation for Economic Co-operation and Development. (2020). *Health data governance: Privacy, monitoring and research*. OECD Publishing.

25. Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. *New England Journal of Medicine, 380*, 1347–1358. https://doi.org/10.1056/NEJMra1814259

26. Rindfleisch, T. C. (2017). Privacy, information security, and health data. *Journal of Biomedical Informatics, 67*, 104–110. https://doi.org/10.1016/j.jbi.2017.01.006

27. Shaw, J., Jamieson, T., Agarwal, P., et al. (2018). Virtual care policy recommendations. *BMJ Open, 8*, e019795. https://doi.org/10.1136/bmjopen-2017-019795

28. Topol, E. (2019). *Deep medicine: How artificial intelligence can make healthcare human again*. Basic Books.

29. World Health Organization. (2019). *Health security and preparedness*. WHO.

30. World Health Organization. (2021). *Ethics and governance of artificial intelligence for health*. WHO.

31. World Health Organization. (2022). *Global strategy on digital health 2020–2025*. WHO.