The Review Of
DIABETIC
STUDIES OPEN ACCESS

Digital Transformation In Healthcare Safety And Prevention: An Interprofessional Health Informatics Framework Involving Nursing, Health Security, Laboratory, Pharmacy, And Public Health

Mohammed Nasser Abdullah Alasmari[1], Mohammed Saad Nasser Al Asmari[2], Moneera mohammed Asiri[3], Ahmed lafi Allogmani[4], Anas Saleh Ahmed emam[5], Salha Hassan Alalwi[6], Yousef Arif Alshammri[7], Razan Fawzi AlManabri[8], Sultan Hassan M Alasmari[9], Saeed Abdullah AL asmary[10], Mohammed Yahya hobish harissi[11], Ibrahim mohammed Yahya khubrani[12], Omar Mohammed Jaber Harisi[13], Hashim Abdullah Alhazmi[14], Mohammed Sulaiman Jubran Huraysi[15]

[1]Long stay hospital and renal care center - Aseer health cluster, Health informatics assistant specialist
[2]Billasmar general hospital - Aseer health cluster, Nurse technician
[3]Aseer centeral hospital, Nursing specialist
[4]Nursing technician, Primary health care center in mulagia
[5]Nursing specialist, Amal hospital Jeddah
[6]Nursing Specialist, Rabigh General Hospital
[7]Health assistant - Health security, Hail Health Cluster
[8]Dental Assistant Specialist, King Fahad General Hospital - Dental Department
[9]Billasmar general hospital - Aseer health cluster, Pharmacist
[10]Billasmar general hospital - Aseer health cluster, Pharmacist
[11]Public Health Technician, vector control center in Al-Ardah
[12]Public Health Technician, vector control center in Al-Ardah
[13]Public Health Technician, vector control center in Al-Ardah
[14]Technician Public Health, Vector Control Center in Alardah
[15]Laboratory Technician, vector control center in Al-Ardah

Abstract

Digital transformation has become a central driver of healthcare safety, prevention, and system resilience. The increasing complexity of care delivery, coupled with emerging infectious threats, medication-related harm, diagnostic errors, and chronic disease burden, has exposed the limitations of fragmented, paper-based, and siloed healthcare systems. Health informatics offers an integrative solution by enabling real-time data capture, interoperability, predictive analytics, and coordinated decision-making across disciplines. This comprehensive narrative review examines digital transformation in healthcare safety and prevention through an interprofessional health informatics framework involving nursing, health security, laboratory services, pharmacy, and public health. Emphasis is placed on clinical surveillance, early warning systems, medication safety, laboratory integration, infection prevention, and population-level risk monitoring. The review highlights how digitally enabled interprofessional collaboration enhances patient safety, strengthens preventive capacity, and supports sustainable health system performance.

Keywords Health informatics; digital health; patient safety; prevention; nursing informatics; laboratory information systems; pharmacy informatics; health security; public health surveillance.

Introduction

Healthcare systems worldwide are undergoing rapid digital transformation driven by escalating patient complexity, workforce constraints, global health threats, and rising expectations for safety and quality.

Traditional healthcare delivery models—characterized by fragmented documentation, delayed information flow, and discipline-specific silos—have proven inadequate for preventing avoidable harm and responding effectively to emerging risks. Patient safety incidents, medication errors, healthcare-associated infections, diagnostic delays, and failures in outbreak detection continue to impose substantial human and economic costs across health systems.

Health informatics has emerged as a foundational enabler of safer and more preventive healthcare. By leveraging electronic health records, clinical decision support systems, laboratory and pharmacy information systems, surveillance platforms, and data analytics, informatics enables timely risk identification, coordinated response, and continuous learning. The World Health Organization has repeatedly emphasized that digital health is essential for strengthening health systems, improving patient safety, and enhancing preparedness for public health emergencies (1,2).

Crucially, the impact of digital transformation depends not only on technology but on interprofessional integration**.** Nursing, health security, laboratory services, pharmacy, and public health each generate and rely on critical data streams that, when digitally connected, create a comprehensive safety and prevention ecosystem. This review explores how an interprofessional health informatics framework can align these disciplines to support proactive risk detection, prevention, and system resilience.

1.1 Global Patient Safety Crisis and the Limits of Traditional Systems

Healthcare safety remains one of the most pressing global public health challenges despite decades of clinical advancement and quality improvement initiatives. Preventable adverse events—including medication errors, diagnostic delays, healthcare-associated infections, and system failures—continue to account for substantial morbidity, mortality, and economic burden worldwide. Conservative estimates suggest that unsafe care ranks among the leading causes of death globally, with millions of patients harmed annually across both high- and low-income health systems (1,2).

Traditional healthcare safety approaches have largely relied on retrospective analysis, such as incident reporting systems, mortality reviews, and root-cause analyses. While these mechanisms provide valuable learning opportunities, they are fundamentally reactive and limited by underreporting, reporting bias, and delayed feedback. Moreover, they operate within disciplinary silos, where nursing, laboratory services, pharmacy, public health, and health security systems often generate safety-critical data independently, without real-time integration.

The increasing complexity of healthcare delivery has further exposed the inadequacy of fragmented safety systems. Aging populations, rising multimorbidity, antimicrobial resistance, global mobility, pandemics, and climate-related health threats demand safety and prevention mechanisms that are predictive**,** integrated, and system-wide rather than episodic and isolated.

1.2 Digital Transformation as a Paradigm Shift in Safety and Prevention

Digital transformation represents a fundamental shift in how healthcare systems conceptualize and operationalize safety. Rather than focusing solely on preventing discrete errors, digital health enables continuous risk surveillance, early signal detection, and coordinated interprofessional response. Health informatics integrates electronic health records, clinical decision support, laboratory and pharmacy information systems, surveillance platforms, and analytics engines into a unified digital infrastructure capable of supporting prevention at scale (3).

The World Health Organization has explicitly recognized digital health as a cornerstone of patient safety, health system resilience, and emergency preparedness, emphasizing that interoperable digital systems are essential for early detection, rapid response, and learning health systems (4,5). Importantly, digital

transformation is not synonymous with technology adoption; rather, it represents a socio-technical transformation that reshapes workflows, professional roles, governance structures, and decision-making processes.

1.3 Interprofessional Nature of Healthcare Safety Data

Healthcare safety data are inherently interprofessional. Nurses continuously generate real-time patient status data; laboratories produce diagnostic and surveillance information; pharmacists manage medication safety signals; public health systems aggregate population-level risk intelligence; and health security units monitor threats that transcend individual facilities. When these data streams remain disconnected, safety intelligence is fragmented and delayed.

Digital health informatics enables the convergence of these data streams, transforming isolated observations into actionable system-level insight. For example, subtle changes in nursing early warning scores combined with abnormal laboratory trends and pharmacy alerts may indicate emerging sepsis risk, antimicrobial resistance, or outbreak signals long before traditional reporting mechanisms detect them.

This convergence necessitates an interprofessional framework that recognizes each discipline as both a producer and consumer of safety data, rather than as passive recipients of centralized information.

1.4 Rationale for an Interprofessional Health Informatics Framework

Most existing digital health implementations remain discipline-centric, focusing on isolated domains such as electronic prescribing, laboratory automation, or nursing documentation. While valuable, such implementations fail to unlock the full preventive potential of digital transformation. Safety emerges not from isolated digital tools but from interoperability, coordination, and shared situational awareness.
An interprofessional health informatics framework aligns nursing, laboratory, pharmacy, health security, and public health data within a shared digital ecosystem governed by common standards, ethics, and accountability structures. This framework enables healthcare systems to move from incident response to anticipatory prevention, from local optimization to system resilience, and from fragmentation to integration.

1.5 Objectives of This Review

This review aims to:

1. Examine the role of digital transformation in enhancing healthcare safety and prevention
2. Analyze discipline-specific informatics contributions from nursing, laboratory, pharmacy, health security, and public health
3. Propose an interprofessional informatics framework for integrated safety and prevention
4. Explore governance, ethical, workforce, and equity implications
5. Provide a foundation for policy, institutional, and academic adoption

Theoretical and Conceptual Foundations of Digital Safety, Prevention, and Health Informatics

2.1 Reframing Healthcare Safety Through Systems Thinking

Healthcare safety has historically been conceptualized through linear causality models that attribute adverse events to individual error or isolated process failures. While such models have contributed to awareness and accountability, they are increasingly inadequate for explaining harm within modern healthcare systems characterized by complexity, interdependence, and constant adaptation. Systems thinking reframes safety as an emergent property of interactions between people, processes, technologies, and organizational structures rather than as the absence of individual mistakes (6).

In this context, digital transformation is not simply a technical upgrade but a systems-level intervention that reshapes how information flows, decisions are made, and risks are managed. Health informatics provides the infrastructure necessary to observe system behavior in real time, enabling healthcare organizations to

detect weak signals of failure before they escalate into harm. By integrating data across nursing, laboratory, pharmacy, health security, and public health domains, informatics supports a holistic view of safety that aligns with contemporary systems-based safety science.

2.2 Safety-I and Safety-II Paradigms in the Digital Era

Traditional patient safety strategies align with the "Safety-I" paradigm, which focuses on identifying what went wrong and preventing recurrence through standardization and control. Incident reporting systems, root cause analyses, and compliance audits exemplify this approach. While valuable, Safety-I is limited by underreporting, hindsight bias, and an emphasis on failure rather than success (7).

The emergence of digital health enables a transition toward the "Safety-II" paradigm, which emphasizes understanding how systems succeed under variable conditions. Safety-II focuses on everyday clinical work, adaptive capacity, and resilience. Digital informatics systems capture routine performance data—nursing observations, laboratory trends, medication workflows, and population surveillance—that reveal how healthcare professionals manage complexity in real time. By analyzing these data streams, health systems can identify conditions that support safe outcomes and replicate them at scale (8).

This paradigm shift is particularly relevant for prevention, where the objective is not merely to avoid harm but to sustain safe functioning across diverse and unpredictable contexts. Digital systems thus become instruments of organizational learning rather than tools of retrospective blame.

2.3 Learning Health Systems and Preventive Intelligence

The concept of the learning health system provides a unifying framework for digital transformation in safety and prevention. Learning health systems continuously collect data from routine care, analyze outcomes, and feed insights back into practice improvement. This cyclical process depends on robust informatics infrastructure, interoperable data sources, and interprofessional collaboration (9).

Preventive intelligence represents an advanced manifestation of the learning health system, wherein data analytics and predictive modeling anticipate risk before adverse events occur. Early warning scores derived from nursing documentation, laboratory trend analysis, pharmacy surveillance, and public health indicators exemplify preventive intelligence in action. These capabilities transform healthcare safety from a reactive endeavor into a proactive, anticipatory discipline.

Importantly, preventive intelligence relies on data integration across disciplines. Isolated datasets rarely provide sufficient context to predict harm. It is the convergence of clinical, diagnostic, medication, and population-level data that enables accurate risk stratification and timely intervention.

2.4 Health Informatics as a Socio-Technical Discipline

Health informatics is inherently socio-technical, encompassing both technological systems and the human actors who design, implement, and use them. Failures in digital health initiatives often stem not from technical deficiencies but from misalignment between systems and clinical workflows, professional roles, or organizational culture (10).

Nursing informatics illustrates this principle clearly. Nurses generate large volumes of safety-critical data, yet poorly designed documentation systems can increase cognitive load, reduce situational awareness, and introduce new error pathways. Similarly, laboratory and pharmacy informatics systems must align with clinical decision-making processes to ensure timely interpretation and action. Effective digital transformation therefore requires participatory design, interprofessional engagement, and continuous usability evaluation.

From a prevention perspective, socio-technical alignment ensures that digital alerts, dashboards, and analytics support rather than disrupt clinical judgment. Informatics systems should augment human expertise, not replace it, preserving professional autonomy while enhancing situational awareness.

2.5 Interoperability as a Safety Imperative

Interoperability—the ability of digital systems to exchange, interpret, and use data across organizational and professional boundaries—is a foundational requirement for integrated safety and prevention. Fragmented systems create informational blind spots that delay detection of emerging risks and hinder coordinated response. Interoperability enables the synthesis of nursing observations, laboratory results, pharmacy data, and public health surveillance into a unified safety intelligence platform (11).

From a theoretical standpoint, interoperability transforms healthcare organizations from loosely coupled units into coordinated networks capable of collective sense-making. This transformation is particularly critical for health security and outbreak prevention, where delays of hours or days can have substantial consequences. Interoperable informatics systems thus function as connective tissue linking frontline care with population-level prevention.

2.6 Human Factors Engineering and Digital Safety

Human factors engineering provides critical insights into how digital systems influence safety. Alert fatigue, automation bias, and cognitive overload are well-documented risks associated with poorly designed informatics tools. These phenomena underscore the necessity of designing digital systems that align with human cognitive capacities and clinical workflows (12).

In an interprofessional informatics framework, human factors considerations extend beyond individual users to team dynamics and organizational processes. Shared dashboards, standardized terminologies, and clear escalation pathways support collective situational awareness and reduce ambiguity. Nursing, laboratory, pharmacy, and public health professionals must be able to interpret and act upon shared data without confusion or delay.

2.7 Ethical Foundations of Digital Safety and Prevention

Digital transformation in healthcare safety raises complex ethical considerations related to data privacy, surveillance, consent, and equity. The use of predictive analytics and population surveillance must balance preventive benefit with respect for individual rights. Ethical governance frameworks are essential to ensure transparency, accountability, and trust (13).

Equity is a central ethical concern. Digital systems that fail to account for social determinants of health risk perpetuating or exacerbating disparities. Conversely, informatics systems that integrate social risk data and support targeted interventions can advance health equity. Ethical digital safety therefore requires intentional design choices that prioritize inclusivity and fairness.

2.8 Conceptual Integration: Toward an Interprofessional Informatics Framework

Synthesizing systems thinking, Safety-II, learning health systems, socio-technical theory, and human factors engineering yields a conceptual foundation for an interprofessional health informatics framework. This framework positions digital systems as enablers of collective intelligence, integrating diverse data streams to support safety and prevention across clinical and population contexts.

Nursing, health security, laboratory, pharmacy, and public health informatics each contribute distinct yet complementary perspectives. When aligned through shared standards, governance, and professional collaboration, these domains form a resilient safety ecosystem capable of adapting to evolving risks.

Nursing Informatics as the Frontline Engine of Digital Safety and Prevention

3.1 Nursing as the Primary Generator of Safety-Critical Data

Nursing practice occupies a uniquely central position within healthcare safety systems because nurses are continuously present at the point of care and are responsible for the most frequent, detailed, and longitudinal clinical observations. Unlike episodic physician encounters or isolated diagnostic events, nursing documentation captures the dynamic evolution of patient status, including subtle physiological changes, behavioral cues, functional decline, and responses to interventions. In the digital era, this continuous stream of nursing-generated data constitutes one of the most valuable sources of safety intelligence within health informatics ecosystems.

Digital nursing documentation—when structured, standardized, and interoperable—transforms routine bedside observations into system-wide early warning signals. Vital signs, pain scores, mental status assessments, intake–output monitoring, and mobility evaluations feed into automated early warning systems capable of detecting clinical deterioration hours before catastrophic events occur. The safety value of these systems is not inherent in the technology itself but in the quality, timeliness, and clinical judgment embedded in nursing data entry. Thus, nursing informatics serves as the frontline engine that powers digital safety and prevention infrastructure (14,15).

3.2 Early Warning Systems and Prevention of Clinical Deterioration

One of the most well-established contributions of nursing informatics to patient safety is the development and implementation of early warning systems. These systems aggregate nursing-entered physiological parameters and generate risk scores that prompt escalation when predefined thresholds are exceeded. Evidence consistently demonstrates that early warning systems reduce rates of unrecognized deterioration, cardiac arrest, unplanned intensive care admissions, and mortality when integrated effectively into nursing workflows (16).

From a prevention perspective, early warning systems exemplify the transition from reactive response to anticipatory care. Nurses not only enter data but also interpret alerts, contextualize them within the patient's clinical narrative, and initiate timely interventions. Importantly, digital systems that fail to incorporate nursing judgment—such as rigid alert thresholds without contextual flexibility—risk alert fatigue and reduced effectiveness. Advanced nursing informatics integrates trend analysis, individualized baselines, and clinical context, reinforcing nurses' role as active safety agents rather than passive data entry points (17).

3.3 Nursing Informatics in Infection Prevention and Control

Infection prevention represents a critical intersection between nursing practice, digital surveillance, and public health safety. Nurses are responsible for implementing and documenting infection control measures, monitoring symptoms, and identifying deviations from expected recovery trajectories. Digital nursing documentation supports infection prevention by enabling real-time tracking of symptoms, isolation status, device use, and adherence to preventive protocols.

When integrated with laboratory and public health systems, nursing informatics contributes to early outbreak detection and containment. For example, clusters of fever, respiratory symptoms, or gastrointestinal complaints documented by nurses may signal emerging infections before laboratory confirmation is available. Digital dashboards that aggregate nursing symptom data across units or facilities enhance situational awareness and enable proactive intervention, reinforcing nursing's role in health security and system resilience (18).

3.4 Chronic Disease Prevention and Longitudinal Safety Monitoring

Beyond acute care, nursing informatics plays a foundational role in chronic disease prevention and long-term safety monitoring. Nurses manage registries for diabetes, hypertension, asthma, and other chronic conditions, ensuring regular follow-up, screening, and adherence to preventive guidelines. Digital registries enable nurses to identify care gaps, track outcomes, and stratify risk across populations.

This longitudinal perspective is essential for prevention, as many safety failures in chronic disease management arise from delayed follow-up, fragmented care, or inadequate monitoring rather than acute error. Nursing informatics systems support proactive outreach, reminder systems, and population-level analytics that reduce preventable complications and hospitalizations. By embedding prevention into routine nursing workflows, digital systems extend safety beyond episodic encounters to sustained population health protection (19).

3.5 Equity-Oriented Nursing Informatics and Social Risk Detection

Health inequities represent a major safety and prevention challenge, as socially disadvantaged populations experience higher rates of preventable harm, delayed diagnosis, and poor outcomes. Nursing informatics contributes to equity-oriented safety by capturing social determinants of health, including housing instability, food insecurity, health literacy limitations, and barriers to care. Nurses are often the first professionals to identify these risks through patient interaction and assessment.

Digitally capturing social risk data enables targeted interventions and informs public health planning. When integrated with clinical, laboratory, and pharmacy systems, social data enhance risk stratification and prevention strategies. Importantly, equity-oriented nursing informatics reframes safety as a population-level responsibility rather than solely an individual clinical outcome, aligning nursing practice with public health prevention principles (20).

3.6 Workflow Integration and Cognitive Safety

The safety impact of nursing informatics depends heavily on workflow integration and cognitive ergonomics. Poorly designed documentation systems increase cognitive load, distract from patient care, and introduce new error pathways. Conversely, systems designed with nursing input enhance situational awareness, reduce duplication, and support decision-making.

Human factors research demonstrates that digital tools must align with nursing workflows to support safety effectively. This includes minimizing redundant data entry, presenting information in intuitive formats, and integrating alerts into natural work patterns. Interprofessional informatics frameworks must recognize nursing workflow as a central design reference point, ensuring that safety tools support rather than disrupt frontline care (21).

3.7 Nursing Leadership in Digital Safety Governance

Nurses play a critical role not only as users of informatics systems but as leaders in digital safety governance. Nursing leadership contributes to system design, policy development, training, and evaluation of digital safety initiatives. Inclusion of nursing perspectives in governance structures ensures that digital transformation remains clinically grounded and patient-centered.

Leadership in nursing informatics also extends to advocacy for safe staffing, adequate training, and ethical data use. Nurses are uniquely positioned to identify unintended consequences of digital systems, such as documentation burden or inequitable access, and to advocate for corrective action. In this way, nursing informatics leadership strengthens both safety outcomes and organizational resilience (22).

3.8 Integration with Interprofessional Safety Ecosystems

Nursing informatics does not operate in isolation; its preventive potential is realized only through integration with laboratory, pharmacy, health security, and public health informatics. Nursing observations contextualize laboratory results, inform medication safety decisions, and enrich surveillance data used for outbreak detection. Interprofessional dashboards and shared analytics platforms enable collective sense-making and coordinated response.

This integration transforms nursing data from localized observations into system-wide safety intelligence. In an interprofessional informatics framework, nursing serves as the connective thread linking individual patient experiences with organizational and population-level prevention strategies. This role positions nursing informatics as a cornerstone of digital safety and preventive healthcare systems.

Laboratory and Pharmacy Informatics as Pillars of Diagnostic and Medication Safety

4.1 Diagnostic Safety as a Core Dimension of Healthcare Prevention

Diagnostic error represents one of the most consequential yet under-recognized threats to patient safety and prevention. Errors may occur at multiple stages of the diagnostic process, including test ordering, specimen collection, analysis, result interpretation, and clinical follow-up. Laboratory medicine underpins a substantial proportion of clinical decisions, and failures within laboratory workflows can cascade into delayed treatment, inappropriate therapy, or missed opportunities for prevention. Digital transformation reframes diagnostic safety by embedding informatics systems that enhance accuracy, timeliness, traceability, and interprofessional communication throughout the diagnostic lifecycle (23).

Laboratory informatics systems serve as the backbone of diagnostic safety by standardizing processes, reducing manual transcription, and ensuring that diagnostic data are available to clinicians in real time. Importantly, the safety value of laboratory informatics extends beyond individual test results to include trend analysis, pattern recognition, and population-level surveillance. When integrated into interprofessional health informatics frameworks, laboratory data become preventive intelligence capable of signaling emerging risks before they manifest as clinical harm.

4.2 Laboratory Information Systems and Error Prevention

Laboratory information systems (LIS) play a central role in preventing diagnostic errors by supporting specimen tracking, test validation, and automated result reporting. Digitally enabled specimen identification reduces mislabeling and loss, while automated checks ensure analytic quality and consistency. These systems significantly reduce pre-analytical and post-analytical errors, which historically account for a large proportion of diagnostic failures (24).

Integration between LIS and electronic health records enhances safety by ensuring that laboratory results are delivered directly to the point of care, reducing reliance on manual communication. Critical value alerts and abnormal trend notifications enable timely clinical response, transforming laboratory data into actionable safety signals. From a prevention standpoint, laboratory informatics reduces diagnostic delay, supports early disease detection, and enables proactive intervention.

4.3 Laboratory Informatics and Antimicrobial Resistance Surveillance

Antimicrobial resistance (AMR) represents a global health security threat with profound implications for patient safety and prevention. Laboratory informatics systems are essential for detecting resistance patterns, monitoring antimicrobial susceptibility trends, and informing stewardship programs. Digitally aggregated laboratory data enable real-time surveillance of resistance emergence at local, national, and global levels (25).

Integration of laboratory informatics with pharmacy and public health systems amplifies preventive capacity. Resistance data inform prescribing decisions, guide infection control measures, and support policy interventions aimed at reducing inappropriate antimicrobial use. Without digital integration, AMR surveillance remains fragmented and delayed, undermining prevention efforts. Thus, laboratory informatics functions as a critical bridge between diagnostic accuracy and population-level health security.

4.4 Pharmacy Informatics and the Medication Safety Lifecycle

Medication-related harm is among the most common causes of preventable patient injury across healthcare systems. Errors may occur during prescribing, dispensing, administration, or monitoring, particularly in complex care environments characterized by polypharmacy and multimorbidity. Pharmacy informatics addresses these vulnerabilities by embedding safety checks across the entire medication lifecycle.

Computerized provider order entry (CPOE) systems with clinical decision support reduce prescribing errors by flagging allergies, contraindications, dosing errors, and drug–drug interactions. Barcode medication administration systems enhance bedside safety by verifying patient identity and medication correctness, significantly reducing administration errors (26). Importantly, pharmacy informatics does not replace clinical judgment but augments it by providing timely, evidence-based guidance at the point of care.

4.5 Medication Safety, Prevention, and Chronic Disease Management

Beyond acute safety, pharmacy informatics contributes to long-term prevention by supporting medication optimization, adherence monitoring, and pharmacovigilance. Chronic diseases such as diabetes, hypertension, and cardiovascular disease require sustained medication management to prevent complications. Pharmacy informatics systems enable population-level monitoring of medication use patterns, identifying gaps in adherence and opportunities for preventive intervention.

Integration with nursing and laboratory data further enhances safety. Laboratory values inform dose adjustments and monitoring for toxicity, while nursing documentation captures patient response and adherence challenges. Interprofessional informatics integration thus transforms medication management from a fragmented process into a coordinated safety and prevention strategy (27).

4.6 Pharmacovigilance and Real-Time Safety Surveillance

Pharmacovigilance traditionally relies on passive reporting of adverse drug events, which is limited by underreporting and delayed recognition. Digital pharmacy informatics enables active surveillance by analyzing large datasets for signals of harm. Automated detection of abnormal laboratory trends, unexpected clinical events, or medication combinations supports early identification of adverse drug reactions and enables rapid response (28).

From a prevention perspective, real-time pharmacovigilance reduces cumulative harm and informs safer prescribing practices. When integrated with public health informatics, pharmacovigilance data contribute to regulatory decision-making and population-level safety interventions. This integration exemplifies how digital transformation extends safety beyond individual care to system-wide prevention.

4.7 Interprofessional Integration of Diagnostic and Medication Safety

Diagnostic and medication safety are deeply interdependent. Laboratory results inform prescribing decisions, while medications influence diagnostic interpretation through side effects and interactions. Digital informatics frameworks that integrate laboratory and pharmacy systems with nursing and clinical workflows enable holistic safety oversight.

Shared dashboards, standardized terminologies, and interoperable data streams support collective situational awareness and coordinated action. For example, rising creatinine levels detected by laboratory informatics combined with pharmacy alerts for nephrotoxic medications prompt timely intervention. This interprofessional integration exemplifies the preventive potential of digital safety ecosystems.

4.8 Ethical and Governance Considerations in Laboratory and Pharmacy Informatics

The expansion of laboratory and pharmacy informatics raises ethical considerations related to data use, algorithm transparency, and patient autonomy. Predictive analytics and automated alerts must be governed by clear policies that ensure accountability and avoid over-reliance on automation. Ethical stewardship requires transparency, clinician engagement, and mechanisms for oversight and continuous evaluation (29).

Governance structures must also address data privacy and cybersecurity, particularly as laboratory and pharmacy systems exchange sensitive information across organizational boundaries. Trust in digital safety systems is essential for sustained adoption and effectiveness.

Health Security and Public Health Informatics: Surveillance, Preparedness, and Population-Level Prevention

5.1 Health Security as a Digital Safety Domain

Health security extends the concept of patient safety beyond individual clinical encounters to encompass population-level protection from infectious diseases, environmental hazards, antimicrobial resistance, and system-wide disruptions. In an increasingly interconnected world, health threats propagate rapidly across borders and care settings, exposing the limitations of traditional surveillance systems that rely on delayed reporting and manual aggregation. Digital transformation has redefined health security by enabling real-

time surveillance, early signal detection, and coordinated response across healthcare, laboratory, and public health domains.

Health informatics functions as the backbone of modern health security, transforming routine clinical and diagnostic data into strategic intelligence. The World Health Organization emphasizes that digital surveillance systems are essential for early detection of outbreaks, monitoring of health threats, and strengthening preparedness at national and global levels (30,31). Importantly, health security informatics is not isolated from clinical care; it relies on data generated by nurses, laboratories, pharmacies, and frontline clinicians, reinforcing the interprofessional nature of preventive safety systems.

5.2 Syndromic Surveillance and Early Threat Detection

Syndromic surveillance represents a foundational component of digital health security, enabling the detection of abnormal health patterns based on symptoms, clinical presentations, and healthcare utilization rather than confirmed diagnoses alone. By aggregating data from emergency departments, primary care, nursing documentation, and laboratory requests, syndromic surveillance systems identify emerging threats earlier than traditional reporting mechanisms (32).

From a prevention perspective, syndromic surveillance shifts health systems from reactive outbreak response to anticipatory action. Early increases in respiratory symptoms, gastrointestinal complaints, or febrile illness documented across care settings may signal emerging infections, environmental exposures, or bioterrorism events. Digital dashboards and automated alerts support rapid situational awareness and facilitate timely public health intervention, reducing transmission and mitigating harm.

5.3 Integration of Clinical and Public Health Informatics

Historically, clinical informatics and public health informatics evolved as separate domains, resulting in fragmented data flows and delayed response. Digital transformation enables convergence between these domains, aligning patient-level data with population-level analytics. Integration allows public health authorities to access timely, high-resolution data while preserving clinical workflows and patient privacy.

This integration enhances preventive capacity by enabling bidirectional data exchange. Clinical data inform public health surveillance, while public health insights guide frontline prevention strategies. For example, identification of rising infection rates through public health analytics prompts targeted screening, vaccination, or infection control measures within healthcare facilities. Interprofessional informatics frameworks thus dissolve traditional boundaries between clinical care and public health, creating a unified safety ecosystem (33).

5.4 Pandemic Preparedness and Digital Resilience

The COVID-19 pandemic exposed critical vulnerabilities in global health security systems, including delays in detection, fragmented data infrastructure, and limited interoperability. Digital health informatics emerged as both a challenge and a solution, highlighting the importance of robust, interoperable systems for surveillance, contact tracing, vaccination tracking, and resource allocation.

Preparedness in the digital era depends on the ability to rapidly scale surveillance, integrate diverse data sources, and support coordinated decision-making across sectors. Health informatics platforms that link clinical, laboratory, pharmacy, and public health data enable real-time assessment of disease spread, healthcare capacity, and intervention effectiveness. These capabilities are essential not only for pandemics but also for seasonal outbreaks, natural disasters, and other health emergencies (34).

5.5 Environmental and Occupational Health Surveillance

Health security informatics extends beyond infectious diseases to include environmental and occupational health threats. Digital systems enable monitoring of air and water quality, heat-related illness, chemical exposures, and workplace hazards, linking environmental data with health outcomes. Integration of these data streams supports early identification of exposure-related health risks and informs preventive action.

Nursing and primary care documentation often provide the first indication of environmental health impacts, such as clusters of respiratory symptoms during pollution events or heat-related illness during extreme

weather. When integrated with public health and environmental informatics, these observations contribute to comprehensive prevention strategies that address upstream determinants of health (35).

5.6 Equity and Vulnerability in Health Security Informatics

Health threats disproportionately affect vulnerable populations, including the elderly, those with chronic conditions, low-income communities, and marginalized groups. Digital health security systems must therefore be designed with equity considerations to avoid reinforcing disparities. Disaggregated data, geospatial analysis, and integration of social determinants of health enable identification of at-risk populations and targeted preventive interventions.

Public health informatics that incorporates equity metrics supports more just and effective responses to health threats. Without such integration, surveillance systems risk masking disparities and perpetuating unequal protection. Equity-oriented health security informatics aligns prevention strategies with broader public health and social justice goals (36).

5.7 Governance, Ethics, and Trust in Public Health Informatics

The expansion of digital surveillance raises ethical concerns related to privacy, consent, data governance, and public trust. Health security informatics must balance the need for timely information with respect for individual rights and community autonomy. Transparent governance structures, clear legal frameworks, and public engagement are essential to maintaining trust and legitimacy.

Ethical stewardship is particularly important during emergencies, when expanded surveillance powers may be justified but must remain proportionate and time-limited. Interprofessional governance models that include clinical, public health, legal, and community perspectives strengthen accountability and ethical decision-making (37).

5.8 Interprofessional Collaboration in Population-Level Prevention

Effective health security informatics depends on sustained interprofessional collaboration. Nurses provide frontline observations; laboratories confirm diagnoses; pharmacies monitor medication supply and safety; public health authorities coordinate response; and health security units manage preparedness and policy. Digital platforms that support shared situational awareness and coordinated action enable these roles to function synergistically.

This collaboration transforms population-level prevention from a fragmented responsibility into a collective endeavor. Interprofessional informatics frameworks thus operationalize the principle that health security is a shared obligation across disciplines and sectors.

Governance, Ethics, Workforce Development, and Equity in Interprofessional Health Informatics

6.1 Governance as the Backbone of Digital Safety and Prevention

Digital transformation in healthcare safety and prevention cannot succeed without robust governance structures that align technology with clinical priorities, ethical standards, and public accountability. Governance defines how data are collected, shared, interpreted, and acted upon across nursing, laboratory, pharmacy, health security, and public health domains. In the absence of coordinated governance, digital systems risk reinforcing silos, generating unsafe workarounds, and undermining trust among professionals and the public.

Effective informatics governance is inherently interprofessional. Safety-critical data traverse multiple domains, and decisions about interoperability standards, access privileges, alert thresholds, and escalation pathways must reflect shared ownership rather than discipline-specific control. Governance bodies that include nursing leaders, laboratory directors, pharmacists, public health officials, health security experts, and informatics specialists are better positioned to align digital systems with real-world workflows and safety goals (38). Such shared governance structures transform informatics from a technical function into a strategic safety instrument.

6.2 Policy Alignment and Regulatory Frameworks

Digital safety and prevention operate within complex regulatory environments shaped by health policy, data protection laws, and international obligations. Policies governing health information exchange, patient privacy, cybersecurity, and surveillance authority directly influence the effectiveness of informatics systems. Regulatory fragmentation—where clinical, laboratory, pharmacy, and public health data are governed by separate and sometimes conflicting rules—creates barriers to integration and delays preventive action.

International frameworks, including those promoted by the World Health Organization, emphasize the need for harmonized digital health governance that supports interoperability, patient safety, and preparedness while safeguarding rights (39,40). Aligning national policies with these frameworks enhances cross-border collaboration, outbreak response, and shared learning. From a prevention perspective, regulatory clarity enables timely data sharing without legal ambiguity, strengthening system resilience.

6.3 Ethical Foundations of Digital Safety Systems

Ethics is central to digital transformation in healthcare safety and prevention. Informatics systems increasingly rely on surveillance, predictive analytics, and automated decision support, raising concerns about consent, transparency, bias, and autonomy. Ethical digital safety frameworks must balance collective benefit with individual rights, ensuring that prevention does not become coercive or discriminatory.

Predictive algorithms used for risk stratification and early warning must be transparent, auditable, and continuously evaluated for bias. If algorithms disproportionately flag certain populations without addressing underlying social determinants, they risk reinforcing inequities rather than preventing harm. Ethical governance requires inclusive design processes, stakeholder engagement, and mechanisms for appeal and correction (41).

Public trust is a fragile yet essential component of digital safety. Without trust, data quality deteriorates, participation declines, and preventive capacity is compromised. Ethical stewardship—grounded in transparency, proportionality, and accountability—is therefore not ancillary but foundational to effective informatics-driven safety systems.

6.4 Data Privacy, Security, and Cyber-Resilience

As healthcare systems become increasingly digital and interconnected, cybersecurity emerges as a critical patient safety issue. Data breaches, ransomware attacks, and system outages disrupt care delivery, compromise confidentiality, and erode public confidence. From a prevention perspective, cybersecurity is inseparable from safety; a compromised system cannot reliably detect risk or support coordinated response.

Interprofessional informatics frameworks must integrate cybersecurity considerations into system design and governance. This includes role-based access control, audit trails, encryption, and contingency planning. Workforce training in cyber hygiene is equally important, as human factors remain a leading cause of security breaches. Cyber-resilient health systems are those that anticipate threats, maintain redundancy, and recover rapidly from disruption, ensuring continuity of safety-critical functions (42).

6.5 Workforce Development and Informatics Competency

Digital transformation redefines professional roles and competencies across healthcare disciplines. Nurses, laboratory professionals, pharmacists, public health practitioners, and health security personnel increasingly rely on informatics tools for decision-making, surveillance, and coordination. Yet workforce readiness remains uneven, with gaps in informatics literacy and confidence posing risks to safety and prevention.

Embedding informatics competencies into pre-service education and continuing professional development is essential. These competencies extend beyond technical skills to include data interpretation, ethical reasoning, interprofessional communication, and systems thinking. Interprofessional training programs foster shared understanding of data flows and safety objectives, reducing miscommunication and enhancing collaboration (43).

Leadership development is particularly important. Clinicians with informatics expertise serve as translators between technical teams and frontline practice, ensuring that digital systems remain aligned with safety goals. Investing in such leadership strengthens organizational capacity for continuous improvement and innovation.

6.6 Equity-Oriented Digital Transformation

Equity considerations must be integral to digital safety and prevention strategies. Digital systems that fail to account for social determinants of health risk perpetuating disparities in access, outcomes, and protection. Conversely, well-designed informatics systems can illuminate inequities and guide targeted interventions.

Equity-oriented informatics integrates social risk data, geospatial analysis, and disaggregated reporting to identify vulnerable populations and tailor preventive strategies. Nurses and public health professionals play key roles in capturing and interpreting these data, translating digital insights into community-based action. Governance structures must ensure that equity metrics are prioritized alongside traditional safety indicators (44).

Digital inclusion is also critical. Populations with limited access to technology or digital literacy may be excluded from preventive interventions if systems are not designed inclusively. Addressing these gaps requires coordinated policy, community engagement, and investment in accessible digital infrastructure.

6.7 Accountability, Measurement, and Continuous Learning

Governance frameworks must include mechanisms for accountability and evaluation. Digital safety initiatives should be continuously monitored for effectiveness, unintended consequences, and equity impact. Metrics should encompass not only incident reduction but also early detection, response timeliness, and population-level outcomes.

Learning health systems thrive on feedback loops that translate data into improvement. Interprofessional informatics governance supports these loops by ensuring that insights are shared across disciplines and incorporated into practice. Accountability is thus reframed from punitive oversight to collective learning and system optimization (45).

6.8 Toward Sustainable and Trusted Digital Safety Systems

Sustainability is a defining challenge for digital transformation. Pilot projects and isolated innovations often fail to scale or endure due to lack of governance alignment, workforce capacity, or funding. Sustainable digital safety systems require long-term vision, institutional commitment, and integration into core health system functions.

Trust—among professionals, patients, and communities—is the ultimate determinant of sustainability. Transparent governance, ethical stewardship, workforce engagement, and equity-oriented design collectively build this trust. When trust is established, digital transformation becomes a shared endeavor rather than an imposed change, enhancing both safety and prevention.

Integrated Discussion: Digital Transformation as a Systemic Engine for Healthcare Safety and Prevention

7.1 From Fragmented Safety Efforts to Systemic Prevention

This review demonstrates that digital transformation in healthcare safety and prevention is not a collection of isolated technological upgrades but a systemic reconfiguration of how health systems perceive, detect, and manage risk. Traditional safety efforts—rooted in retrospective incident analysis and discipline-specific interventions—are fundamentally misaligned with the complexity of modern healthcare. Errors, outbreaks, diagnostic failures, and medication harm do not arise from single points of failure but from dynamic interactions among professionals, technologies, workflows, and populations. The evidence synthesized across nursing, laboratory, pharmacy, health security, and public health domains confirms that safety emerges as a property of the system rather than the performance of any individual component.

Health informatics enables a paradigmatic shift from reactive harm mitigation **to** anticipatory prevention by integrating data streams that were historically siloed. When nursing observations, laboratory diagnostics,

pharmacy data, and population surveillance are digitally connected, health systems acquire the capacity to recognize weak signals of failure before they escalate into adverse events. This shift aligns with contemporary safety science, which emphasizes resilience, adaptability, and learning rather than error counting alone.

7.2 Nursing Informatics as the Anchoring Layer of Digital Safety

Across all domains examined, nursing informatics consistently emerges as the anchoring layer of digital safety systems. Nurses generate the most continuous, context-rich clinical data, capturing patient trajectories that are invisible to episodic encounters or single diagnostic tests. Early warning systems, infection surveillance, chronic disease registries, and equity-oriented assessments all depend on high-quality nursing documentation. The discussion across prior sections underscores that digital safety systems succeed not because data exist, but because nursing data are timely, interpretable, and embedded within meaningful workflows.

Importantly, nursing informatics operationalizes Safety-II principles by capturing how care succeeds under variable conditions. Rather than focusing solely on deviations and errors, nursing data reveal adaptive strategies, early compensations, and contextual judgment that sustain safe care. When informatics systems are designed with nursing leadership and human-factors principles, they enhance rather than constrain professional expertise, strengthening prevention rather than generating alert fatigue or documentation burden.

7.3 Diagnostic and Medication Safety as Interdependent Processes

A central insight of this review is that diagnostic safety and medication safety cannot be meaningfully separated in digital safety frameworks. Laboratory informatics and pharmacy informatics form a tightly coupled subsystem in which diagnostic interpretation directly informs prescribing decisions, and medications in turn alter laboratory values and clinical trajectories. Digital integration enables bidirectional safety intelligence: abnormal trends prompt medication review, while prescribing alerts contextualize diagnostic findings.

The discussion highlights that isolated digital interventions—such as standalone laboratory systems or electronic prescribing—deliver only partial safety gains. Preventive impact emerges when laboratory trends, pharmacy alerts, and nursing observations converge within shared dashboards and escalation pathways. This interdependence reinforces the necessity of interprofessional governance and shared accountability for safety outcomes.

7.4 Health Security and Public Health Informatics as Preventive Multipliers

Health security and public health informatics expand the scope of safety from individual patients to entire populations. Syndromic surveillance, antimicrobial resistance monitoring, and environmental health data transform routine clinical encounters into population-level preventive intelligence. The integration of clinical and public health data dissolves artificial boundaries between care delivery and prevention, enabling rapid detection of emerging threats and coordinated response.

The COVID-19 pandemic serves as a stark illustration of both the potential and the fragility of digital health security systems. Where interoperable informatics infrastructures existed, surveillance and response were accelerated; where fragmentation prevailed, delays amplified harm. The synthesis presented in this discussion emphasizes that preparedness is not episodic but continuous, requiring sustained integration of nursing, laboratory, pharmacy, and public health data streams. Digital transformation thus becomes a cornerstone of national and global health security strategies endorsed by organizations such as the World Health Organization.

7.5 Governance as a Determinant of Safety Outcomes

A recurring theme across all sections is that governance—not technology—is the decisive factor in determining whether digital transformation improves or undermines safety. Informatics systems redistribute power, visibility, and responsibility; without shared governance, these shifts can create new

risks. Interprofessional governance structures align digital priorities with clinical realities, ethical principles, and public accountability.

This discussion reinforces that effective governance must operate across multiple levels: organizational, regional, and national. Policies governing interoperability, data sharing, cybersecurity, and ethical use must be coherent and aligned. Fragmented regulation not only delays preventive action but also erodes trust among professionals and communities. Conversely, transparent and inclusive governance enables digital systems to function as trusted safety infrastructure rather than surveillance tools.

Conclusion

This comprehensive review demonstrates that digital transformation in healthcare safety and prevention represents a fundamental reconfiguration of how health systems anticipate, detect, and manage risk. Rather than functioning as isolated technological enhancements, digital health informatics systems—when designed and governed interprofessionally—form a safety and prevention infrastructure that reshapes clinical practice, public health surveillance, and system resilience. Across nursing, laboratory services, pharmacy, health security, and public health, informatics emerges not as a support function but as a core determinant of safety performance.

A central conclusion of this work is that safety is an emergent, system-level property rather than the outcome of individual vigilance or compliance alone. Fragmented safety strategies, siloed data systems, and retrospective incident analysis are insufficient in healthcare environments characterized by complexity, uncertainty, and rapid change. Digital transformation enables a shift toward anticipatory prevention, in which early signals of risk are detected through integrated data streams and acted upon through coordinated interprofessional response.

Nursing informatics is shown to be the foundational layer of digital safety systems. Nurses generate the most continuous and context-rich clinical data, enabling early detection of deterioration, infection risk, and care gaps. When nursing documentation is digitally structured and interoperable, it fuels early warning systems, infection surveillance, chronic disease prevention, and equity-oriented interventions. Importantly, nursing informatics operationalizes contemporary safety science by capturing how care succeeds under variable conditions, supporting resilience rather than blame.

Laboratory and pharmacy informatics function as critical pillars of diagnostic and medication safety. Digital laboratory systems reduce diagnostic error, accelerate clinical response, and support antimicrobial resistance surveillance, while pharmacy informatics embeds safety checks across the medication lifecycle and enables real-time pharmacovigilance. The integration of laboratory, pharmacy, and nursing data transforms isolated safety checks into holistic prevention mechanisms, reducing cumulative harm and improving long-term outcomes, particularly in multimorbidity and chronic disease management.

Health security and public health informatics expand safety beyond individual patients to populations and societies. Syndromic surveillance, outbreak detection, environmental health monitoring, and preparedness analytics convert routine healthcare data into preventive intelligence. The integration of clinical and public health informatics dissolves traditional boundaries between care delivery and prevention, enabling rapid response to emerging threats and strengthening system resilience. Global experiences—including pandemics and antimicrobial resistance—underscore that preparedness is continuous and digitally enabled, not episodic or reactive.

Governance, ethics, and workforce development emerge as decisive enablers—or barriers—to successful digital transformation. Technology alone does not produce safety; safety arises from ethical stewardship, shared governance, informatics literacy, and public trust**.** Interprofessional governance structures ensure alignment between digital systems and clinical realities, while ethical frameworks safeguard privacy, equity, and transparency. Workforce readiness, including informatics competency and interprofessional training, determines whether digital systems enhance or undermine safety.

Equity is reaffirmed as a core safety outcome rather than a secondary consideration. Digitally enabled safety systems that fail to incorporate social determinants of health risk reproducing inequities at scale. Conversely, informatics systems that integrate social risk data and support targeted prevention enable more

just and effective health protection. Nursing and public health informatics play particularly critical roles in translating digital insights into community-level action.

In synthesis, this review establishes that digital transformation in healthcare safety and prevention is most effective when implemented as an interprofessional, socio-technical, ethically governed system. An integrated health informatics framework involving nursing, laboratory services, pharmacy, health security, and public health enables proactive risk detection, coordinated response, and population-level prevention. Investment in interprofessional informatics capacity is therefore essential for building safer, more resilient, and more equitable health systems capable of meeting contemporary and future challenges.

References:

1. World Health Organization. Global strategy on digital health 2020–2025. Geneva: WHO.
2. World Health Organization. Patient safety and digital health. Geneva: WHO.
3. World Health Organization. International Health Regulations (2005): Monitoring and evaluation framework. Geneva: WHO.
4. World Health Organization. Strengthening preparedness through digital health. Geneva: WHO.
5. World Health Organization. Global antimicrobial resistance surveillance system (GLASS). Geneva: WHO.
6. Bates DW, Cohen M, Leape LL, Overhage JM, Shabot MM, Sheridan T. Reducing the frequency of errors in medicine using information technology. J Am Med Inform Assoc.
7. Sheikh A, Anderson M, Albala S, et al. Health information technology and digital innovation for patient safety. Lancet Digit Health.
8. Friedman CP, Wong AK, Blumenthal D. Achieving a nationwide learning health system. Health Aff.
9. Friedman CP, Rubin JC, Sullivan KJ. Toward an information infrastructure for global health. J Am Med Inform Assoc.
10. Reason J. Human error: models and management. BMJ.
11. Hollnagel E, Wears RL, Braithwaite J. From Safety-I to Safety-II: A White Paper.
12. Braithwaite J, Wears RL, Hollnagel E. Reconceptualizing patient safety. BMJ Qual Saf.
13. Vincent C. Patient Safety. 2nd ed. Wiley-Blackwell.
14. Carayon P, Wetterneck TB, Hundt AS, et al. Human factors in health information technology. Qual Saf Health Care.
15. Sittig DF, Singh H. A sociotechnical approach to health IT safety. BMJ Qual Saf.
16. McGonigle D, Mastrian KG. Nursing Informatics and the Foundation of Knowledge.
17. Topaz M, Murga L, Gaddis KM, et al. Nursing informatics and patient safety. J Nurs Care Qual.
18. Sensmeier J. Leadership in nursing informatics. Nurs Adm Q.
19. Smith ME, Chiovaro JC, O'Neil M, et al. Early warning systems for detecting clinical deterioration. BMJ.
20. Downey CL, Tahir W, Randell R, Brown JM, Jayne DG. Strengths and limitations of early warning scores. Resuscitation.
21. Buehler JW, Hopkins RS, Overhage JM, Sosin DM, Tong V. Syndromic surveillance systems. MMWR Suppl.
22. Yasnoff WA, O'Carroll PW, Koo D, et al. Public health informatics. J Public Health Manag Pract.
23. Bodenheimer T, Wagner EH, Grumbach K. Improving primary care for chronic illness. JAMA.
24. Wagner EH, Austin BT, Von Korff M. Organizing care for patients with chronic illness. Milbank Q.
25. Marmot M, Allen J, Bell R, Bloomer E, Goldblatt P. WHO review of social determinants of health. Lancet.
26. Krieger N. Health equity and population surveillance. Am J Public Health.
27. Singh H, Meyer AND, Thomas EJ. Diagnostic error in healthcare. BMJ Qual Saf.
28. Plebani M. Diagnostic errors and laboratory medicine. Clin Chem Lab Med.
29. Kaushal R, Shojania KG, Bates DW. Effects of computerized prescribing on medication errors. JAMA.

30. Carter BL, Rogers M, Daly J, Zheng S, James PA. Pharmacist-led interventions in chronic disease management. Arch Intern Med.
31. Harpaz R, DuMouchel W, Shah NH, et al. Data mining for adverse drug events. Clin Pharmacol Ther.
32. Keesara S, Jonas A, Schulman K. Covid-19 and healthcare's digital revolution. N Engl J Med.
33. Frumkin H, Hess J, Luber G, et al. Climate change and environmental health informatics. Annu Rev Public Health.
34. Gostin LO, Friedman EA, Wetter SA. Responding to public health emergencies. JAMA.
35. Reeves S, Pelone F, Harrison R, Goldman J, Zwarenstein M. Interprofessional collaboration. Cochrane Database Syst Rev.
36. Floridi L, Cowls J, Beltrametti M, et al. AI ethics in healthcare. Philos Trans A Math Phys Eng Sci.
37. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare. JMIR Med Inform.
38. Hersh W. Health informatics education and workforce development. Methods Inf Med.
39. Donabedian A. Evaluating the quality of medical care. Milbank Q.
40. Berwick DM. Continuous improvement as an ideal in healthcare. N Engl J Med.
41. Vincent C, Amalberti R. Safer Healthcare: Strategies for the Real World. Springer.
42. Braithwaite J. Changing how we think about healthcare safety. BMJ.
43. Adler NE, Glymour MM, Fielding J. Addressing social determinants in healthcare. JAMA.
44. Frenk J, Chen L, Bhutta ZA, et al. Health professionals for a new century. Lancet.
45. Greenhalgh T, Wherton J, Papoutsi C, et al. Beyond adoption: digital health transformation. J Med Internet Res.