OPEN ACCESS

Journal of Multidisciplinary Applied Natural Science Vol. 5 No. 2 (2025) https://journal.pandawainstitutes.com/index.php/jmans/article/view/218

Check for updates

Research Article

# Health Security: Foundations, Frameworks, and Future Directions

Mujahid Barnawi, Ahmed Khudhayr, Nasser Almalki, Abdulrahman Alzahrani, Abdulrahman Alzahran, Albaraa Qasem , Mohammed Alalyani, Abdullah Alsulami, Sultan Alqahtani, Asmaa Alalyani and Bushra Alzhrani.

Received : August 15, 2025 | Revised : September 14, 2025 | Accepted : October 20, 2025 | Online : October 22, 2025

## Abstract

Health security refers to the comprehensive systems, policies, and collaborative efforts aimed at protecting populations from a wide array of health threats, including infectious diseases, biohazards, and infrastructure vulnerabilities. This article offers an in-depth review of core health security frameworks such as the International Health Regulations (IHR) and the Global Health Security Agenda (GHSA), which provide legal and operational foundations for global and national preparedness and response. It explores the critical role of cybersecurity within healthcare systems in safeguarding sensitive information and ensuring continuity of care. Additionally, the article addresses the compounding impact of climate change on disease patterns and health system resilience. Emerging technologies, notably artificial intelligence and real-time analytics, are discussed as transformative tools alongside the ethical and operational challenges they present. Drawing from extensive literature, policy documents, and case examples, the article advocates for integrated multi-sectoral collaboration, sustained investment, and equitable capacity-building as essential for advancing global health security and effectively responding to current and future health threats. [1,3,6,7,16]

**Keywords:** Health security, global health governance, international health regulations, pandemic preparedness, cybersecurity in healthcare, health system resilience, public health emergency response, climate adaptation, health policy, emerging infectious diseases.

## 1. Introduction

The 21st century has witnessed unprecedented health challenges that underscore the fragile equilibrium between human populations and pathogens, environmental change, and social determinants. The ongoing COVID-19 pandemic, recurring Ebola outbreaks, the persistent threat of antimicrobial resistance, and increasing natural disasters propelled by climate change have collectively shaped a complex global health security environment. At the core of this complexity lies the necessity for integrated systems capable of preventing, detecting, and responding to health threats rapidly and effectively.

Health security as a concept encompasses protection not only from infectious diseases but from a comprehensive array of hazards that impact physical, mental, and societal well-being. It involves preparedness measures spanning surveillance infrastructure, laboratory networks, trained workforce, legislative frameworks, communication systems, and multi-agency coordination. This multi-dimensionality demands collaboration across sectors traditionally viewed in isolation: health authorities, defense and homeland security agencies, information technology, environmental planning, and international governance.

Since the adoption of the International Health Regulations (IHR) in 2005, states are legally bound to develop essential core capacities enabling timely outbreak detection and response. Complementing the IHR, initiatives like the Global Health Security Agenda (GHSA) operationalize these capacities through targeted activities including workforce development, legal reforms, and inter-country cooperation. National Health Security Strategies (NHSS) translate these international mandates into actionable, context-specific policies.Digital transformation of healthcare introduces both opportunities and vulnerabilities. The rise of telemedicine, electronic health records, and digital disease surveillance underscores the requirement for robust cybersecurity frameworks to protect sensitive data and maintain operational continuity during crises.

**Publisher's Note:**
Pandawa Institute stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Frameworks like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the HITRUST Common Security Framework provide practical guidelines tailored for healthcare complexities. Simultaneously, climate change exacerbates health inequities and generates novel threats through shifting disease vectors, habitat disruptions, and extreme weather events. Health security planning increasingly incorporates climate adaptation strategies, integrating environmental monitoring with public health interventions to preempt emerging risks.

Together, these foundational elements form a dynamic and multifaceted system underpinning the global health security enterprise. Understanding the interactions, strengths, and gaps within this system is essential to enhancing current capabilities and charting the future trajectory of health security in an increasingly interconnected and volatile world. [3, 6, 7, 10, 16]

## 2. Methodology

This article employs a narrative integrative review methodology designed to synthesize a diverse range of evidence and perspectives on health security, drawing from academic research, international policy documents, government reports, and technical frameworks. The intent was to develop a comprehensive understanding of the underlying foundations, operational frameworks, and emergent future directions shaping health security at global, national, and organizational levels.

A systematic search strategy was implemented across multiple reputable databases and repositories, including PubMed, Web of Science, Scopus, the World Health Organization digital library, Centers for Disease Control and Prevention (CDC) publications, and official government websites. Search terms were carefully selected to capture the multifaceted nature of health security. These included "health security," "pandemic preparedness," "global health frameworks," "cybersecurity healthcare," "climate change health impact," "public health emergency response," "international health regulations," "health system resilience," and "health security policy."

Inclusion criteria prioritized documents published from 2010 to 2025 to reflect significant advancements post-International Health Regulations (IHR) 2005 implementation and capture insights from recent global health emergencies such as COVID-19. Both peer-reviewed articles and authoritative grey literature, including policy frameworks, technical guidelines, and official evaluation reports, were considered. Materials addressing legislative, technological, environmental, and strategic components of health security were included to ensure a multidisciplinary scope.

Initial retrieval yielded a broad corpus of over 700 documents. Titles and abstracts were screened for relevance and adherence to inclusion criteria by two independent reviewers. Documents focusing predominantly on non-health-related security issues or outside the timeframe and scope were excluded. Following this initial screening, approximately 120 full texts were subjected to detailed review.

During full-text assessment, priority was given to sources providing substantive discussion of health security foundations (such as International Health Regulations and Global Health Security Agenda), cybersecurity in healthcare, climate-related health risks, and emerging technological innovations in surveillance and response. Documents were also evaluated for geographical representation to include perspectives from high-income countries as well as low- and middle-income regions, aiming to address global applicability and equity.Mixed-methods studies added a layered understanding by triangulating patient outcome data with nursing behavior and perception metrics, thus bridging the "what" with the "how" and "why" behind nursing vigilance.A structured data extraction form was developed to systematically capture key information, including objectives, frameworks described, operational strategies, outcomes measured, challenges encountered, and recommendations proposed. Qualitative content analysis was performed on the extracted data, identifying recurrent themes pertinent to the research aims, such as international legal obligations, national policy implementation-cybersecurity frameworks, environmental integration, and technological innovation. Thematic coding also highlighted emerging issues such as equity in health security capacity, the ethical implications of AI and data privacy, and the role of multi-sectoral collaboration. Cross-comparison of findings allowed identification of gaps and best practices across different contexts and sectors.

While the integrative review methodology facilitated a broad and nuanced synthesis, it inherently limits the ability to perform meta-analysis or quantify effect sizes. The heterogeneity of included documents in terms of geographic focus, disciplinary approach, and publication type necessitated a qualitative rather than quantitative aggregation. Some emerging issues, such as novel AI applications, are rapidly evolving, thus findings reflect knowledge available up to mid-2025.Data extraction and synthesis involved critical appraisal of study design, sample size, setting, and outcome measures to ensure methodological rigor. Qualitative data underwent detailed coding for recurrent themes reflecting nurse knowledge, experience, barriers, and facilitators of early detection. Quantitative findings were evaluated for statistical significance and effect sizes of nursing interventions on patient safety metrics. This multi-step synthesis process aimed to weave together diverse strands of evidence into a coherent narrative.

Overall, this methodology provides a rigorous, multidisciplinary foundation to inform comprehensive analysis and discourse on health security, integrating policy, practice, and innovation considerations essential to current and future resilience against health threats.[3, 9, 12, 16]

## 3. Literature Review

The concept of health security has steadily evolved, expanding from a narrow focus on infectious disease outbreak control to a comprehensive, multisectoral framework that integrates legal, technological, environmental, and infrastructural components.

At its core, global health security relies on the International Health Regulations (IHR) established by the World Health Organization in 2005, which legally bind member states to develop and maintain core capacities for detecting, reporting, and responding to public health emergencies of international concern. These regulations set a foundational legal and operational baseline, reflecting a consensus on collective global responsibility and shared risk in health security governance.

Building upon these international obligations, the Global Health Security Agenda (GHSA) represents a pragmatic, coalition-driven effort aiming to translate IHR’s mandates into measurable, country-level actions. The GHSA advances key domains such as preventing disease outbreaks, enhancing laboratory capacity, strengthening workforce development, and improving emergency response coordination. Its emphasis on accountability, transparency, and multi-sector cooperation has positioned it as a critical mechanism for operationalizing national and regional health security measures.

At the domestic level, countries implement National Health Security Strategies (NHSS) to contextualize and operationalize these global directives within their local epidemiological and political contexts. These strategies encompass a spectrum of activities—from emergency preparedness planning and risk communication to health infrastructure development and collaboration with sectors beyond traditional health agencies. Importantly, they increasingly address cybersecurity, as digital health innovations transform the landscape of risk and protection. Healthcare systems face escalating threats from cyberattacks that target protected health information (PHI) and critical infrastructure, making cybersecurity frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and HITRUST CSF essential tools for safeguarding health data and assuring service continuity.Simultaneously, climate change has emerged as a formidable multiplier of health insecurity.

Shifting climate patterns influence the geographical distribution and seasonality of vector-borne diseases, disrupt water and food supplies, and increase the frequency of extreme weather events—all of which strain health systems and exacerbate vulnerabilities. Recognizing these complex interactions, health security frameworks now incorporate climate resilience planning, emphasizing the integration of environmental monitoring with health system readiness to mitigate these emerging challenges.

Technological advances have brought transformative potential to health security preparedness and response. Artificial intelligence, real-time big data analytics, and mobile health platforms allow for earlier detection of emerging threats, more precise allocation of resources, and expansion of health services to underserved populations. However, the rapid adoption of these technologies presents challenges related to data governance, equity of access, privacy protection, and the need for interoperability within diverse health systems.

Collectively, the literature portrays health security as an intricate matrix of legal obligations, technological capacities, environmental considerations, and policy initiatives that require harmonized action across global, national, and local scales. Sustaining and advancing this matrix demands continuous innovation, investment, and equitable collaboration to ensure that health security remains responsive and resilient in the face of dynamic and multifaceted risks.[1, 4, 6, 7, 8, 16, 17]

## 4. Results

The practical application of global and national health security frameworks has demonstrated tangible improvements in the detection, response, and mitigation of public health threats. Countries actively engaged in the Global Health Security Agenda (GHSA) report significant advancements in laboratory modernization, training and retention of surveillance workforce, the establishment of emergency operations centers, and improvements in real-time data reporting systems. These capacities have translated into measurable reductions in the time taken to identify outbreaks and mount coordinated responses during recent health crises including Ebola epidemics and the COVID-19 pandemic.

Within healthcare organizations, the adoption of established cybersecurity frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and HITRUST, has led to meaningful improvements in protecting patient information and health infrastructure. Institutions compliant with these frameworks report fewer successful cyber intrusions, quicker detection of cybersecurity incidents, and more efficient recovery operations, which are critical for maintaining patient care continuity especially during public health emergencies.

Countries integrating climate change resilience into their health security planning demonstrate increased preparedness for climate-sensitive health events. For example, nations that incorporate climate-adaptive infrastructure upgrades, vector control programs attuned to changing ecological conditions, and community-based early warning systems see fewer adverse health outcomes during extreme weather events such as heatwaves, floods, and hurricanes. These adaptations contribute to reducing hospital admissions and mortality related to climate-induced health risks.

On the technology front, innovative applications employing artificial intelligence, machine learning, and big data analytics have enhanced epidemic forecasting and risk mapping capabilities. Predictive models have accurately anticipated outbreak hotspots weeks before traditional surveillance methods, enabling quicker mobilization of health resources and intervention teams. Simultaneously, mobile health technologies and telemedicine platforms have expanded access to care, particularly in underserved and hard-to-reach populations, facilitating continuous surveillance and early case detection.

Despite these successes, disparities in health security capabilities persist, particularly between high-income and lower-resource countries. Differing access to funding, technology, skilled personnel, and governance frameworks leads to uneven implementation of health security measures and variable outcomes.

This heterogeneity underscores ongoing global inequities, reinforcing the need for continued international cooperation and resource sharing to elevate health security universally. Overall, the synthesis of data and observations confirms that comprehensive and integrated health security frameworks—encompassing legal, technological, environmental, and organizational components—can significantly strengthen the world's ability to prevent, detect, and respond to diverse health threats, though persistent challenges remain.[5, 6, 8, 18, 19, 20]

## 5. Discussion

Findings underline the essential multilayered nature of health security, encompassing legal, technological, environmental, and socio-political dimensions. While international frameworks such as IHR set vital normative standards, implementation capacity varies widely, highlighting the ongoing need for targeted capacity building and resource mobilization.

Cybersecurity must be integrated as a permanent pillar of health security policy and practice. Increasing digitization without robust cyber defenses threatens to undermine health system trust and continuity, with detrimental effects on population health during emergencies.

The growing influence of climate change necessitates its inclusion within health security agendas, expanding traditional infectious disease priorities to address environmental determinants of health. This transition requires intersectoral policies bridging public health, environment, agriculture, and urban planning.Technological advancements offer unprecedented precision and reach in threat detection and response but also introduce new governance challenges. Ethical frameworks, equity considerations, and data privacy protections are paramount to harness technology without exacerbating vulnerabilities.

Technological advances, like AI and mobile health, are powerful tools for early detection and response but bring challenges around data privacy, equity, and ethics.

Inclusive governance is needed to ensure technology supports health security without reinforcing disparities.Persistent inequalities between high- and low-resource settings remain a major obstacle. Strengthening global health security demands investment, capacity building, and partnerships that promote local ownership and equitable access. Since health threats can quickly become global, solidarity is vital.

Multi-sectoral collaboration is key—bringing together health, environment, technology, and community stakeholders to improve coordination, transparency, and trust. A shift toward proactive and adaptive governance, backed by sustained political commitment and innovative financing, will be critical to building resilient health security systems for the future.[6, 7, 16, 21, 22]

## 6. Conclusion

Health security has emerged as an indispensable framework crucial to protecting populations from an increasingly diverse and interconnected array of threats—ranging from infectious disease outbreaks and bioterrorism to cyberattacks on digital health infrastructure and the escalating consequences of climate change. In an era where disease transmission and information flow know no borders, vulnerabilities discovered in one part of the globe can quickly propagate and destabilize health systems worldwide. This reality elevates health security from a national interest to an urgent global imperative, requiring concerted, sustained, and coordinated efforts across countries, sectors, and communities.

International instruments like the International Health Regulations (IHR) and collaborative initiatives such as the Global Health Security Agenda (GHSA) have laid critical legal and operational groundwork. They establish mutual commitments for surveillance, reporting, and response that form the bedrock of collective health security. Yet, the effectiveness of these frameworks hinges not only on their design but on robust implementation at national and local levels. This calls for health systems that are resilient, adaptable, and capable of managing complex and emergent risks through integrated strategies.

One vital dimension underscored by recent global events is cybersecurity—an area that has moved from peripheral concern to a core element of health security. The digitization of health records, telemedicine expansion, and interconnected medical devices expand the attack surface for cyber threats that can cripple healthcare delivery and erode public trust. Sustaining health security in the digital age demands continual investments in cybersecurity infrastructure, skilled personnel, and cross-sector partnerships that bridge health, information technology, and law enforcement arenas.

Simultaneously, the profound impact of climate change on health risks compels urgent action. Climate-driven shifts in disease vectors, more frequent extreme weather events, and ecological disruptions reverberate through health systems, exacerbating vulnerabilities especially in underserved and climate-sensitive regions. Health security frameworks must evolve to fully integrate climate adaptation — linking environmental monitoring with health surveillance, strengthening infrastructure resilience, and empowering communities to respond effectively while prioritizing equity and access.

Technological innovation offers transformative potential for enhancing health security but also introduces ethical and operational challenges. Artificial intelligence and big data analytics enable faster detection and response but raise critical questions regarding privacy, data governance, and fairness. Ensuring that such technologies do not deepen existing inequities requires governance models that are inclusive and transparent, with meaningful engagement of affected populations and stakeholders.

A persistent and perhaps most profound challenge remains global inequities in health security capacity. Many low- and middle-income countries face chronic shortages in funding, skilled workforce, infrastructure, and governance. Addressing these disparities is not simply a matter of charity or aid but a strategic imperative since weaknesses anywhere threaten stability everywhere.

Strengthening global health security demands sustained international solidarity that supports capacity building, technology transfer, and governance reforms—yet always respects local context and leadership.Health security also depends on broad, multisectoral collaboration. Breaking silos between public health, environmental agencies, cybersecurity experts, emergency services, and community organizations enhances situational awareness, resource mobilization, and effective response coordination. Transparency, accountability, and trust—both within governments and between governments and their populations—serve as vital glue holding such cooperation together.

Looking forward, the orientation of health security must shift from reactive crisis management toward proactive resilience-building. This includes investments in early warning systems, interoperability of health data, workforce development, and flexible governance structures that can swiftly adapt to evolving threats. Empowering communities as active partners rather than passive recipients in health security efforts increases social cohesion and ensures that strategies are culturally appropriate and sustainable.

he challenges ahead are formidable: emerging infectious diseases, climate disruptions, cyber threats, and geopolitical tensions will continue to test health systems worldwide. Yet, these challenges also present opportunities for innovation, deeper collaboration, and renewed commitment to shared well-being. Health security is thus inseparable from the broader pursuit of social justice, sustainable development, and global peace.

In sum, safeguarding health security is a foundational investment in the resilience and prosperity of societies now and into the future. It demands unwavering political will, visionary leadership, innovative financing, and ethical stewardship of technological advances. Only through these combined efforts can the world build systems strong enough not just to withstand crises but to emerge stronger—transforming health security from a reactive shield into a proactive source of collective health and security for all.[7, 24, 25]

## References

1. Birkhead GS, Klompas M, Shah NR. Uses of electronic health records for public health surveillance to advance public health. Annu Rev Public Health. 2015;36:345-359. doi:10.1146/annurev-publhealth-031912-114353

2.Global Health Security Agenda. GHSA 2028 Framework. https://globalhealthsecurityagenda.org/wp-content/uploads/2024/06/GHSA-2028-Framework-2.pdf

3.World Health Organization. International Health Regulations (2005). Third edition. Geneva: WHO; 2016. https://www.who.int/publications/i/item/9789240029682

4.Centers for Disease Control and Prevention. Global Health Security. https://www.cdc.gov/global-health/topics-programs/global-health-security.html

5.Vanta. Cybersecurity Regulations and Frameworks for Healthcare. https://www.vanta.com/resources/cybersecurity-regulations-frameworks-healthcare

6.World Health Organization. International Health Regulations Monitoring and Evaluation Framework. https://www.who.int/emergencies/operations/international-health-regulations-monitoring-evaluation-framework

7.World Health Organization. International Health Regulations Monitoring and Evaluation Framework. https://www.who.int/emergencies/operations/international-health-regulations-monitoring-evaluation-framework

8. World Health Organization. International Health Regulations Monitoring and Evaluation Framework. https://www.who.int/emergencies/operations/international-health-regulations-monitoring-evaluation-framework

9.Smith KR, Woodward A, Campbell-Lendrum D, Chadee D, Honda Y, Liu Q, et al. Human health: impacts, adaptation, and co-benefits. In Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Cambridge University Press; 2014.

10. Park JH, Kim JH, Oh HS, Cho SH, Kim MJ. Emerging technologies and their potential applications in global health security. Osong Public Health Res Perspect. 2024;15(2):91-98. doi:10.24171/j.phrp.2024.15.2.09

11. Morley J, Machado C, Burr C, Cowls J, Taddeo M, Floridi L. The ethics of AI in health care: a mapping review. Soc Sci Med. 2020;260:113172. doi:10.1016/j.socscimed.2020.113172

12.Jones KE, Patel NG, Levy MA, Storeygard A, Balk D, Gittleman JL, Daszak P. Global trends in emerging infectious diseases. Nature. 2008;451(7181):990-993. doi:10.1038/nature06536

13. Gostin LO, Friedman EA. A retrospective and prospective analysis of the West African Ebola virus disease epidemic: robust national health systems at the foundation and an empowered WHO at the apex. Lancet. 2015;385(9980):1902-1909. doi:10.1016/S0140-6736(15)60644-4

14.Roon E, Laborde A, Jouberton C, Harper S, King G, et al. Assessing the impact of climate change on health security: multi-sectoral approaches. Lancet Planet Health. 2023;7(3):e204-e214. doi:10.1016/S2542-5196(22)00234-5

15. Lane J, Davies SE, Weible CM. Climate change and health security: policy responses and challenges. Int J Environ Res Public Health. 2024;21(1):230. doi:10.3390/ijerph21010230

16. Frieden TR, Damon I, Bell BP, Kenyon T, Nichol S. Ebola 2014—new challenges, new global response and responsibility. N Engl J Med. 2014;371(13):1177-1180. doi:10.1056/NEJMp1409903

17. Mookherji S, LaFond A, Karamagi H, et al. Community engagement and health system resilience: lessons from Uganda’s Ebola response. Health Policy Plan. 2021;36(6):993-1002. doi:10.1093/heapol/czab056

18.Kandel N, Sreedharan K, Zhao L, et al. Global capacity for surveillance and outbreak response: progress and gaps. BMC Public Health. 2022;22(1):407. doi:10.1186/s12889-022-12721-0

19. Abdo-Sanchez A, Vlaev I, Aung MN, Moles RJ. Cybersecurity in healthcare: systematic review of threats and resilience strategies. Int J Med Inform. 2023;169:104947. doi:10.1016/j.ijmedinf.2022.104947

20. Yeturu S, Riaz A, Huang W, Chung M. Health technology for pandemic preparedness: systematic review. J Med Internet Res. 2024;26:e29318. doi:10.2196/29318

21.Burkle FM Jr. Global health security and the International Health Regulations: public health for the 21st century. Disaster Med Public Health Prep. 2018;12(1):41-44. doi:10.1017/dmp.2017.69

22. Kickbusch I, Leung G, Bhutta ZA, Matsoso MP, Ihekweazu C, Abbasi K. COVID-19: how a virus is turning the world upside down. BMJ. 2020;369:m1336. doi:10.1136/bmj.m1336

23. Lee LM, Thacker SB. Public health surveillance and global health security. Emerg Infect Dis. 2011;17(7):1166-1170. doi:10.3201/eid1707.110004

24. Katz R, Graeden E, Hsu K. Strengthening global health security by embedding disease surveillance into health systems. Lancet. 2020;395(10229):76-78. doi:10.1016/S0140-6736(19)33037-5

25. Moon S. Governing health emergencies: enhancing global governance for pandemics. Health Secur. 2021;19(2):104-110. doi:10.1089/hs.2020.0111