Engineering Law and Cybersecurity in Digital Health: Legal-Informatics Frameworks for Regulating Cross-Border Data Interoperability, Liability, and Resilience in Public Health Communication Systems

Dr. Grace Perpetual Dafiel[1], Samira Umar Balarabe[2]

[1]Veritas University Nigeria, Abuja

[2]LLM, BL, LLB. Kaduna State University

DOI: https://doi.org/10.51244/IJRSI.2025.1215000139P

Received: 20 August 2025; Revised: 02 September 2025; Accepted: 05 September 2025; Published: 03 October 2025

ABSTRACT

The proliferation of digital health technologies and public health informatics has transformed healthcare delivery and global health governance by enabling real-time data exchange, precision interventions, and transnational collaboration. Yet, these innovations also expose critical vulnerabilities in cybersecurity, liability allocation, and regulatory coherence. This article investigates these challenges through the lens of engineering law, proposing a legal-informatics framework for governing cross-border data interoperability and resilience in public health communication systems. The central research problem addressed is how engineering law—traditionally applied to physical infrastructures—can be reimagined to regulate digital health platforms in ways that embed *safety-by-design, compliance-by-architecture,* and *accountability-by-default* into system development and governance. Methodologically, the study employs a comparative legal analysis of the European Union, United States, and China, combined with socio-technical evaluation of interoperability standards, liability models, and resilience mechanisms. Primary legal instruments (e.g., GDPR, HIPAA, NIS2 Directive, Cybersecurity Law of China), international standards (ISO/IEC 27001, HL7 FHIR, IEC 62443), and case studies (e.g., the EU Digital COVID Certificate, African CDC data platforms) form the empirical basis of the analysis. The findings demonstrate that fragmented legal frameworks and inconsistent liability regimes undermine the resilience of digital health infrastructures, leaving systems vulnerable to cyber threats and regulatory fragmentation. To address these shortcomings, the article proposes a four-pillar regulatory model grounded in interoperability, cybersecurity safeguards, liability allocation, and resilience mechanisms. By operationalising these pillars, the study contributes a novel legal-informatics framework that strengthens both accountability and systemic security. Ultimately, the article offers policymakers, engineers, and legal scholars a structured blueprint for harmonising digital health regulation, advancing transnational public health resilience, and safeguarding trust in an increasingly interconnected digital healthcare ecosystem.

Keywords: Cybersecurity, Digital Health, Engineering Law, Interoperability, Liability, Public Health Informatics, and Resilience

INTRODUCTION

The rapid expansion of digital health technologies and public health informatics has reconfigured global healthcare systems by enabling real-time data exchange, precision-driven interventions, and transnational collaboration. Platforms such as telemedicine, electronic health records (EHRs), and interoperable health data infrastructures now underpin disease surveillance, epidemiological modelling, and international crisis responses. The COVID-19 pandemic exemplified their indispensability, where secure and rapid cross-border data flows facilitated vaccine development, coordinated policy interventions, and genomic surveillance.[1]

[1] COVID-19 vaccines: development, evaluation, approval and monitoring https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/coronavirus-disease-covid-19/covid-19-public-health-emergency-international-concern-2020-23/covid-19-vaccines-development-evaluation-approval-monitoring

However, the same innovations have exposed systemic vulnerabilities: fragmented regulatory frameworks, insufficient cybersecurity resilience, and unsettled liability doctrines threaten both operational stability and public trust when sensitive health data traverse borders.[2]

Engineering law, historically rooted in the governance of physical infrastructures such as transport, energy, and construction, must now be extended to digital infrastructures. Embedding *safety-by-design*, *compliance-by-architecture*, and *accountability-by-default* into the governance of digital health requires integrating legal norms with technical and engineering practices.[3] Such a legal-informatics synthesis is crucial to ensure that public health communication systems remain not only efficient but also secure, rights-compliant, and globally interoperable.

The European Union's **European Health Data Space (EHDS) Regulation (EU) 2025/327** illustrates this convergence by mandating interoperable infrastructures such as *MyHealth@EU*, grounded in the European Interoperability Framework.[4] Yet interoperability is only as robust as its cybersecurity underpinnings. Technical safeguards—including network security, encryption, and access control—must be complemented by governance mechanisms such as identity management, consent protocols, audit logging, and continuity planning.[5] Broader instruments, including the General Data Protection Regulation (GDPR),[6] the EU's NIS2 Directive,[7] the ISO/IEC 27001 standard,[8] and the NIST Cybersecurity Framework,[9] establish layered protections to preserve confidentiality, integrity, and availability of health data. The proposed **EU Cyber Resilience Act** further operationalises *secure-by-default* principles, extending engineering law into digital product governance.[10]

Despite these advances, liability allocation remains unsettled. Failures in EHR systems, AI-assisted diagnostics, and telehealth platforms may trigger claims in negligence, malpractice, or product liability. Although cybersecurity insurance and contractual mechanisms are emerging to distribute risks, the absence of harmonised doctrines creates accountability gaps in multi-actor, cross-border infrastructures.[11] These uncertainties discourage innovation, inhibit trust, and complicate cross-jurisdictional cooperation.

Global divergences exacerbate these difficulties. The European Union foregrounds individual rights, data portability, and interoperability, while China's **Cybersecurity Law (2016)** and **Data Security Law (2021)** prioritise localisation and state control, allowing only limited data exports under strict conditions.[12] By contrast, the United States emphasises sectoral regulation and voluntary coordination; for example, the **Cybersecurity Information Sharing Act 2015** promotes threat intelligence exchange but leaves unresolved

[2] Aidatul Fitriyah and Daryna Abdulovna, 'EU's AI Regulation Approaches and Their Implication for Human Rights' (2024) 7 *Media Iuris* 417, doi:10.20473/mi.v7i3.62050

[3] Gary Marchant, Braden Allenby and Joseph Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Vol 7, Springer 2011) https://doi.org/10.1007/978-94-007-1356-7

[4] Regulation (EU) 2025/327 on the European Health Data Space [2025]. https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

[5] ENISA, *Guidelines for Securing Health Data Infrastructures* (European Union Agency for Cybersecurity 2023). https://www.enisa.europa.eu/

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[7] Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2 Directive) [2022] OJ L333/80. https://www.springlex.eu/packages/nis2/nis2-directive/

[8] International Organization for Standardization, *ISO/IEC 27001: Information Security Management Systems* (ISO, 2022). https://www.iso.org/standard/27001

[9] National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (NIST, 2023). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[10] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

[11] Clelia Casciola, 'Artificial Intelligence and Health Care: Reviewing the Algorithmic Accountability Act in Light of the European Artificial Intelligence Act' (2022) 47 *Vermont Law Review* 127 https://lawreview.vermontlaw.edu/wp-content/uploads/2023/03/06_Casciola_Book1_Final-copy.pdf

[12] Cybersecurity Law of the People's Republic of China (2016) https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ ; Data Security Law of the People's Republic of China (2021). http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html

tensions between liability, privacy, and innovation.[13] This fragmented governance landscape demonstrates the urgent need for a harmonised legal-informatics framework that bridges sovereignty claims with global health imperatives.

Existing scholarship has examined digital health governance in relation to interoperability,[14] cybersecurity,[15] and liability,[16] yet often in isolation. Few studies integrate these dimensions into a coherent legal-informatics model that treats resilience as a regulatory principle rather than a purely technical consideration. This study fills that gap by advancing a four-pillar model—interoperability law, cybersecurity safeguards, liability allocation, and resilience mechanisms—that extends engineering law into digital health infrastructures.

The central argument is that engineering law can and must be adapted to digital systems, embedding enforceable duties into design processes and aligning liability thresholds with engineering standards. The study's contributions are threefold: (i) developing a *safety-by-architecture* ethos that bridges legal doctrines of negligence and liability with technical standards such as IEC 62443; (ii) proposing governance tools—including contractual allocation and insurance models—that strengthen accountability in cross-border contexts; and (iii) providing policymakers, engineers, and legal scholars with a blueprint for resilient, interoperable, and legally accountable digital health infrastructures.

By situating digital health governance within a unified legal-informatics framework, this article offers a novel roadmap for building resilient, rights-respecting, and secure public health systems capable of withstanding the cyber and regulatory challenges of the twenty-first century.

LITERATURE REVIEW

Digital health governance lies at the intersection of law, engineering, and informatics—domains that have advanced rapidly yet often in disciplinary isolation. A thematic synthesis of the literature reveals progress within each field, but also persistent gaps that demand an integrated legal-informatics framework. These would be discussed as follows

Law and Interoperability

Interoperability is widely recognised as a cornerstone of digital health governance, particularly for cross-border services such as e-prescriptions, patient summaries, and genomic surveillance.[17] However, legal coherence across jurisdictions remains elusive. Legal interoperability requires not only technical standards but also alignment of privacy rules, access control, liability doctrines, and professional accreditation.[18]

In the European Union, the **General Data Protection Regulation (GDPR)** operationalises data portability and access rights, while the forthcoming **European Health Data Space (EHDS)** embeds interoperability obligations directly into EU law.[19] This marks a shift from voluntary technical adoption to mandatory legal

[13] Cybersecurity Information Sharing Act 2015, Pub L No 114-113, 129 Stat 2936. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

[14] Kola Adegoke, Abimbola Adegoke, Deborah Dawodu, Ayoola Bayowa and Akorede Adekoya, *Interoperability in Digital Healthcare: Enhancing Consumer Health and Transforming Care Systems* (Preprints 20 February 2025) https://doi.org/10.20944/preprints202502.1774.v1.

[15] Indra Döhmann, 'The Legal Framework for Access to Data from a Data Protection Viewpoint – Especially under the GDPR' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (Nomos 2021) 175–208

[16] Dariusz Kloza, Thibaut D'hulst and Malik Aouadi, What could possibly go wrong? On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification, Technology and Regulation, 2024, 309-329. https://doi.org/10.26116/techreg.2024.022. ISSN: 2666-139X.

[17] Kola Adegoke, Abimbola Adegoke, Deborah Dawodu, Ayoola Bayowa and Akorede Adekoya, *Interoperability in Digital Healthcare: Enhancing Consumer Health and Transforming Care Systems* (Preprints 20 February 2025) https://doi.org/10.20944/preprints202502.1774.v1

[18] Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020)

[19] Regulation (EU) 2025/327 (n 4)

compliance. Scholars argue that legal interoperability frameworks must balance transparency, liability, and trust in transnational contexts.[20] In Africa, systematic reviews of Health Information Exchange (HIE) strategies emphasise enterprise architectures and data governance but highlight that legal frameworks frequently lag behind technical planning.[21]

By contrast, the United States relies on sector-specific regulation under the **Health Insurance Portability and Accountability Act (HIPAA)**, supplemented by voluntary standards adoption.[22] China's **Cybersecurity Law** and **Data Security Law** impose strict localisation and sovereignty-based restrictions, complicating cross-border data flows.[23] These divergent approaches demonstrate how fragmented legal frameworks undermine global interoperability, reinforcing the need for harmonised legal-informatics structures.

Informatics and Standards

The informatics literature has extensively documented interoperability standards for electronic health records (EHRs). HL7 and its derivative FHIR (Fast Healthcare Interoperability Resources) are widely adopted, with FHIR offering modular, API-driven interoperability suited to cloud-based and mobile health systems.[24] Systematic reviews reveal persistent challenges, however, as heterogeneous data formats, inconsistent coding practices, and governance misalignments continue to obstruct seamless integration.[25]

SNOMED CT, LOINC, and ICD-11 contribute standardised terminologies, yet technical convergence remains slow and uneven across regions.[26] Moreover, standards adoption is often shaped by institutional or national priorities rather than international coordination. This has produced a patchwork of "siloed systems" that limit the potential of large-scale initiatives such as genomic surveillance networks or AI-driven diagnostics. Scholars stress that informatics standards must be embedded in enforceable legal frameworks to overcome these barriers.[27]

Engineering and Cybersecurity

The field of health systems engineering applies complex systems methodologies, originally developed for industrial optimisation, to healthcare infrastructures. This includes workflow optimisation, patient safety systems, and interoperability architectures.[28] Engineering perspectives highlight system resilience, redundancy, and fault tolerance as essential for robust health data infrastructures.

Cybersecurity scholarship adds a further dimension. Emerging concepts such as **cyberbiosecurity** explore vulnerabilities at the interface of life sciences and digital infrastructures, including risks of ransomware, data poisoning, and adversarial attacks on AI-enabled medical devices.[29] Regulatory analysis underscores that instruments like the EU's **NIS2 Directive** and **Cyber Resilience Act** attempt to codify *secure-by-design* principles, though harmonisation at the global level remains limited.[30] Scholars argue that compliance-oriented

[20] Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (OUP 2020)

[21] Adane Mamuye et., el., 'Health Information Exchange Policy and Standards for Digital Health Systems in Africa: A Systematic Review' (2022) 1 *PLOS Digital Health* e0000118 https://doi.org/10.1371/journal.pdig.0000118

[22] Health Insurance Portability and Accountability Act 1996, Pub L No 104-191, 110 Stat 1936

[23] Cybersecurity Law of the People's Republic of China (2016) (n 12)

[24] Roberta Gazzarata and others, 'HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in Digital Healthcare Ecosystems for Chronic Disease Management: Scoping Review' (2024) 189 *International Journal of Medical Informatics* 105507 https://doi.org/10.1016/j.ijmedinf.2024.105507 (pubmed.ncbi.nlm.nih.gov)

[25] Vishwasrao Salunkhe, Pattabi Rama Rao Thumati, Pavan Kanchi, Akshun Chhapola and Om Goel, 'EHR Interoperability Challenges Leveraging HL7 FHIR for Seamless Data Exchange in Healthcare' (2013) *Darpan International Research Analysis* https://doi.org/10.36676/dira.v12.i3.98.

[26] WHO, *International Classification of Diseases 11th Revision (ICD-11)* (2022)

[27] Döhmann, 'The Legal Framework for Access to Data from a Data Protection Viewpoint (n. 15)

[28] Lingzhi Li, Shuni Liao, Jingfeng Yuan, Endong Wang and Jianjun She, 'Analyzing Healthcare Facility Resilience: Scientometric Review and Knowledge Map' (2021) 9 *Frontiers in Public Health* 764069 https://doi.org/10.3389/fpubh.2021.764069

[29] Noran Fouad, 'Cyberbiosecurity in the New Normal: Cyberbio Risks, Pre-Emptive Security, and the Global Governance of Bioinformation' (2024) 9 *European Journal of International Security* 1 https://doi.org/10.1017/eis.2024.19

[30] Directive (EU) 2022/2555 (n 7)

security frameworks are insufficient unless complemented by resilience-oriented governance that prioritises continuity and recovery in crises.[31]

Computational Law and Accountability

Computational law research explores the automation of legal processes and the integration of normative structures into digital systems. Automated adjudication, regulatory software, and "compliance-by-code" mechanisms raise unique accountability concerns when deployed in healthcare contexts.[32] Cybersecurity vulnerabilities in such systems highlight the risks of adversarial manipulation and legal uncertainty.

Scholars have argued that embedding legal norms directly into system architectures—through auditability, explainability, and traceability mechanisms—is essential to ensure accountability in AI-driven health governance.[33] Liability analysis emphasises that traditional doctrines of negligence and product liability are poorly suited to distributed, algorithmically mediated health systems where causal attribution is opaque.[34] This literature therefore calls for innovative legal-informatics models that align responsibility allocation with engineering standards and system design.

Identified Gaps

The literature across law, informatics, engineering, and computational governance reveals important progress but remains fragmented. Legal scholarship tends to emphasise rights protection and privacy but rarely engages with the operational realities of technical standards. Informatics research advances interoperability protocols yet often neglect compliance with legal obligations. Engineering studies focus on resilience and fault tolerance but seldom integrate liability allocation or normative frameworks. Computational law scholarship highlights vulnerabilities in automated systems but lacks comprehensive proposals for cross-border digital health governance.

This fragmentation leaves critical gaps:

- Interoperability is treated as a technical aspiration rather than a binding legal duty
- Cybersecurity is addressed through compliance checklists rather than resilience-oriented regulation
- Liability allocation remains unclear in distributed, multi-actor systems
- Resilience is under-theorised as a regulatory principle rather than a technical add-on.

Addressing these gaps requires a **unified legal-informatics-engineering framework** that operationalises *safety-by-design*, embeds resilience into law, and bridges sovereignty with transnational health imperatives. It is this ambition that grounds the present study.

Theoretical And Conceptual Framework

This study advances a four-pillar legal-informatics framework for governing digital health infrastructures: **interoperability, cybersecurity, liability, and resilience**. Each pillar reflects both a normative requirement of law and a functional necessity of engineering, thereby offering a holistic model that embeds *safety-by-design*, *compliance-by-architecture*, and *accountability-by-default* into public health informatics.

Interoperability as Legal Duty and Technical Condition

Interoperability is conventionally defined as the ability of systems to exchange and make use of information. In health informatics, it is operationalised through standards such as HL7 FHIR, ICD-11, SNOMED CT, and

[31] European Union Agency for Cybersecurity (ENISA), *Threat Landscape: Health Sector* (2023). https://www.cybersecitalia.it/wp-content/uploads/2023/07/1688557664622.pdf

[32] Daniel Martin Katz, Michael Bommarito and Josh Blackman, 'A General Approach for Predicting the Behaviour of the Supreme Court of the United States' (2017) 12 *PLoS ONE* 4

[33] Karen Yeung, Andrew Howes and Ganna Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing' (2019) *SSRN Electronic Journal* https://doi.org/10.2139/ssrn.3435011

[34] Dariusz Kloza, et,.el., What could possibly go wrong? (n.16)

LOINC.[35] Yet from a legal-theoretical perspective, interoperability must be reconceptualised as a *binding obligation* rather than a voluntary aspiration.[36]

The European Health Data Space (EHDS) marks a paradigmatic shift by embedding interoperability into EU secondary legislation, thereby transforming a technical challenge into a normative duty enforceable by law.[37] Legal scholars argue that such regulatory embedding operationalises the principle of **functional equivalence**: ensuring that digital health systems can function across borders with equivalent safeguards as physical infrastructures.[38]

Thus, interoperability forms the first pillar: a dual requirement that health data systems not only "speak the same technical language" but also comply with transnational legal harmonisation.

Cybersecurity as Governance by Design

Cybersecurity is not merely a technical safeguard but a normative principle that determines the legitimacy of digital health governance. Failures in cybersecurity—ranging from ransomware attacks on hospitals to data breaches in vaccination databases—undermine public trust and expose systemic vulnerabilities.[39]

Engineering scholarship emphasises **secure-by-design** and **defence-in-depth** approaches, integrating security features into system architectures rather than retrofitting them after deployment.[40] Legally, the EU's **NIS2 Directive** and **Cyber Resilience Act** codify obligations of risk management, incident reporting, and supply-chain assurance, embedding cybersecurity into regulatory governance.[41]

Cyberbiosecurity literature further extends this perspective by highlighting threats at the intersection of biology and informatics, including genome editing tools, synthetic biology data, and AI-driven diagnostics.[42] These risks demonstrate that cybersecurity cannot be reduced to compliance checklists but must be embedded into governance as an ongoing process of **adaptive risk management**.

Accordingly, cybersecurity constitutes the second pillar: a principle that integrates legal norms, technical standards, and adaptive governance into a single continuum of "governance by design."

Liability as Accountability Architecture

Liability remains one of the least developed aspects of digital health governance. Traditional tort doctrines—such as negligence or product liability—are ill-suited to distributed, algorithmically mediated systems where causation is opaque.[43] Emerging discussions around AI liability, including the European Commission's proposed **AI Liability Directive**, attempt to rebalance evidentiary burdens and allocate responsibility in complex socio-technical systems.[44]

From an engineering perspective, liability can be conceptualised as an **accountability architecture**, whereby responsibilities are mapped onto system functions in advance, ensuring that legal duties correspond to technical roles. Computational law research suggests that compliance-by-code mechanisms, audit trails, and explainable AI can provide traceability essential for attributing fault.[45]

[35] Roberta Gazzarata and others, 'HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in Digital Healthcare Ecosystems for Chronic Disease Management: Scoping Review' (2024) 189 *International Journal of Medical Informatics* 105507 https://doi.org/10.1016/j.ijmedinf.2024.105507 (pubmed.ncbi.nlm.nih.gov)
[36] Döhmann, 'The Legal Framework for Access to Data from a Data Protection Viewpoint (n. 15)
[37] Regulation (EU) 2025/327 (n 4)
[38] Hildebrandt, *Law for Computer Scientists (n.20*)
[39] ENISA, *Threat Landscape: Health Sector*. (n. 31)
[40] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd edn, Wiley 2020)
[41] Directive (EU) 2022/2555 (n.7)
[42] Noran Fouad, 'Cyberbiosecurity in the New Normal (n.29)
[43] Dariusz Kloza, et,.el., What could possibly go wrong? (n.16)
[44] European Commission, *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)* COM (2022) 496 final
[45] Karen Yeung, et., el., (n.33)

This pillar thus bridges legal doctrine with system design: liability must evolve from post hoc adjudication into ex ante allocation of accountability embedded into infrastructures.

Resilience as Normative Principle

Resilience—defined as the capacity of systems to withstand, adapt to, and recover from disruptions—has become a central concept in engineering and complex systems theory.[46] Yet in legal scholarship, resilience remains under-theorised, often treated as an operational aim rather than a normative principle.

In public health governance, resilience encompasses both **technical redundancy** (ensuring continuity in case of cyberattack or failure) and **institutional adaptability** (ensuring legal systems can adjust to unforeseen crises, as seen during COVID-19).[47] The World Health Organization (WHO) now advocates resilience-building as a cornerstone of health system governance, but operationalisation at the legal level remains limited.[48]

Resilience, therefore, is conceptualised here as the fourth pillar: a legal-informatics principle that complements cybersecurity by emphasising continuity and adaptive governance. Unlike static compliance regimes, resilience requires law and engineering to co-evolve, embedding adaptability into regulatory frameworks and system architectures alike.

The four pillars—**interoperability, cybersecurity, liability, and resilience**—are interdependent rather than discrete. Interoperability without cybersecurity invites systemic exploitation; cybersecurity without liability undermines accountability; liability without resilience risks rigid systems unable to adapt to crises; and resilience without interoperability leads to fragmented responses.

This framework therefore advances an integrated model of **digital health governance under engineering law**, whereby legal norms and engineering principles are co-constitutive. The contribution is twofold:

1. Conceptually, it reframes engineering law as a discipline capable of governing digital infrastructures, not merely physical ones.
2. Practically, it offers a structured blueprint for policymakers, engineers, and regulators to harmonise digital health governance at transnational scales.

METHODOLOGY

This study employs a comparative legal analysis combined with a case study approach to investigate the governance of digital health infrastructures under the proposed four-pillar legal-informatics framework: interoperability, cybersecurity, liability, and resilience. The methodology is designed to capture both the normative diversity of legal systems and the practical realities of their implementation in public health informatics.

Comparative Legal Analysis

The first strand of methodology involves comparative legal analysis across three major jurisdictions: the European Union, the United States, and China. These regions were selected because they represent divergent regulatory philosophies:

- The European Union foregrounds data protection, interoperability, and rights-based governance, exemplified by the GDPR, the NIS2 Directive, and the newly adopted European Health Data Space Regulation.[49]

[46] Ibid
[47] WHO, *Building Health System Resilience for Universal Health Coverage and Health Security during the COVID-19 Pandemic and Beyond* (2021). https://iris.who.int/bitstream/handle/10665/346515/WHO-UHL-PHC-SP-2021.01-eng.pdf
[48] WHO, (n.47)
[49] Regulation (EU) 2025/327 (n.4)

- The United States adopts a sectoral, market-driven model, with instruments such as the Cybersecurity Information Sharing Act 2015 and the Health Insurance Portability and **Accountability Act (HIPAA)**, supplemented by voluntary guidance frameworks such as the **NIST Cybersecurity Framework 2.0**.[50]
- **China** prioritises data sovereignty and state control, embodied in the **Cybersecurity Law 2016** and the **Data Security Law 2021**, which restrict transnational data flows and impose localisation requirements.[51]

Comparative analysis allows the study to map convergences (e.g. common adoption of risk management frameworks), divergences (e.g. portability vs localisation), and **regulatory blind spots** (e.g. unresolved liability in AI-driven diagnostics). This method situates the four-pillar framework within global governance debates and identifies prospects for harmonisation.

Case Study Approach

The second strand involves case study analysis of concrete digital health infrastructures. These are selected for their global salience, diversity of governance arrangements, and relevance to the four-pillar model:

- **The EU Digital COVID Certificate (EUDCC)**: A pan-European infrastructure enabling cross-border recognition of vaccination and testing records, grounded in the principle of interoperability. It illustrates how legal mandates (through EU Regulations) can drive technical standardisation but also exposes vulnerabilities in data security and liability allocation during pandemic-scale rollouts.[52]
- **The African Centres for Disease Control and Prevention (Africa CDC)**: A regional institution coordinating pandemic response, which has adopted digital surveillance and contact tracing platforms. The Africa CDC highlights challenges of building resilience in contexts with uneven legal frameworks, limited cybersecurity capacity, and strong reliance on donor-driven digital tools.[53]
- **Genomic Surveillance Networks (e.g. GISAID)**: Global databases facilitating real-time sharing of viral genome sequences, instrumental during COVID-19. These systems exemplify both the promise of interoperability and the tensions between open science, data sovereignty, and liability for misuse or misinterpretation of data.[54]

The case study approach is instrumental rather than exhaustive: the selected cases serve as analytical lenses through which the four-pillar framework can be tested, refined, and evaluated in practice.

Normative-Analytical Orientation

The methodology is primarily doctrinal—interpreting statutes, directives, regulations, and case law—while also drawing on interdisciplinary insights from engineering and informatics to ensure technical accuracy. This reflects the law-in-context approach, situating legal frameworks within the socio-technical infrastructures they regulate.[55]

Doctrinal sources (EU Regulations, US federal statutes, Chinese cybersecurity legislation) are read alongside soft-law instruments (NIST Framework, ISO/IEC 27001, WHO resilience strategies) and scholarly commentary. This blended method allows both the black-letter law and the operational realities of digital health infrastructures to be captured.

Limitations

Two limitations are acknowledged. First, the comparative scope, while covering three global regulatory paradigms, does not exhaustively analyse other emerging jurisdictions (e.g. India, Brazil, ASEAN), though

[50] NIST, *Cybersecurity Framework 2.0* (n.9)
[51] Cybersecurity Law (n.12)
[52] European Commission, *EU Digital COVID Certificate.* https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en
[53] John Nkengasong and Wessam Mankoula, 'Looming Threat of COVID-19 Infection in Africa: Act Collectively, and Fast' (2020) 395 *The Lancet* 841
[54] GISAID, *Global Initiative on Sharing All Influenza Data* (2023) https://gisaid.org
[55] Geoffrey Samuel, *An Introduction to Comparative Law Theory and Method* (Hart 2014)

these may be referenced where instructive. Second, as legal-informatics is a fast-evolving domain, regulatory developments (such as pending AI liability legislation in the EU) may shift during or after the study. These limitations are mitigated by focusing on structural principles (the four pillars) that remain relevant across jurisdictions and time.

Justification of Methodological Choice

The integration of comparative legal analysis and case study methodology ensures both breadth (through jurisdictional diversity) and depth (through infrastructure-specific analysis). This dual approach is well suited to testing the four-pillar framework, which requires both normative generalisation and empirical grounding.

This analysis applies the four-pillar framework—interoperability, cybersecurity, liability, and resilience—to three case studies and compares regulatory approaches in the EU, US, and China, establishing a two-level comparative perspective.

Application of the Four-Pillar Framework to Case Studies

Case Study	Interoperability	Cybersecurity	Liability	Resilience
EU Digital COVID Certificate (EUDCC)	Legally mandated under Regulation (EU) 2021/953, harmonising vaccination and testing certificates across 27 states. Shared QR code and public key infrastructure operationalised interoperability as law, though national disparities persisted.	Strong encryption and digital signatures were used, but vulnerabilities arose (e.g. falsified certificates, compromised keys). The NIS2 Directive later embedded mandatory reporting obligations.	Liability allocation remained unclear. While Member States bore issuance duties, responsibility for damages—especially where private actors were intermediaries—was undefined.	Demonstrated adaptive potential beyond COVID-19 (e.g. e-prescriptions). Yet sustainability depends on political will and ongoing technical maintenance.
Africa CDC Digital Platforms (PanaBIOS, Trusted Travel)	Sought cross-border interoperability, but absence of a binding continental framework led to fragmentation. Reliance on donor-driven tools raised concerns about sustainability and sovereignty.	Cybersecurity capacity varied widely; weak funding and expertise meant security-by-design was often sacrificed. No enforceable mandate required states to adopt minimum protections.	Liability frameworks were virtually absent. Heavy reliance on private contractors created gaps in accountability and recourse for affected individuals.	Institutional resilience was evident in cross-state coordination. Technological resilience was fragile, dependent on external vendors and offshore cloud services, raising sovereignty issues.
Genomic Surveillance Networks (GISAID)	Enabled global interoperability through standardised metadata and real-time variant tracking. Yet tensions arose between open science principles and national data sovereignty, particularly in LMICs.	No major breaches reported, but reliance on centralised infrastructure created concentration risks. Governance and security audits remain opaque.	Liability for errors in genomic data use is undefined. GISAID's terms of use disclaim responsibility, leaving accountability gaps for data misuse or misinterpretation.	Successfully scaled during COVID-19, handling vast genomic data. However, disputes over transparency and access restrictions highlighted institutional fragility.

Comparative Application of the Four-Pillar Framework: EU, US, and China

Jurisdiction	Interoperability	Cybersecurity	Liability	Resilience
European Union (EU)	Interoperability embedded in binding law (e.g. EHDS, EUDCC). Legal codification ensures system-wide alignment across Member States despite capacity gaps.	Strong regional baseline under GDPR and NIS2 Directive. Security obligations legally enforceable, though harmonisation across states remains uneven.	Liability addressed partially through sectoral instruments, but cross-border distributed infrastructures still create gaps. Efforts toward shared responsibility models are emerging.	Institutional and technological resilience reinforced through anticipatory governance and adaptive frameworks. Yet continuity depends on political consensus and sustained technical investment.
United States (US)	Fragmented, sector-specific interoperability (e.g. HIPAA, ONC standards). Absence of binding nationwide framework leads to inconsistent adoption and limited cross-state integration.	Cybersecurity largely reliant on voluntary frameworks (NIST). Binding rules are sectoral and reactive, producing uneven baseline protections.	Liability fragmented across state and federal regimes; limited clarity in digital health contexts. Accountability often shifts to private actors without systemic safeguards.	Institutional resilience depends on decentralised federalism, with adaptive innovation in some states but systemic fragility at the national level due to lack of coordination.
China	Prioritises sovereignty over interoperability. Strong state-centric control of data flows restricts cross-border exchange, undermining global alignment.	Cybersecurity embedded in centralised legal frameworks (Cybersecurity Law, Data Security Law). Strong enforcement capacity but oriented toward state security rather than global collaboration.	Liability frameworks remain opaque; state dominance reduces transparency. Individuals have limited avenues for redress, with accountability subordinated to sovereignty imperatives.	Resilience grounded in centralised command-and-control capacity. While effective in crisis mobilisation, it is highly dependent on political will and lacks independent institutional safeguards.

FINDINGS

Comparative analysis across the EU, US, China, and Africa demonstrate that legal frameworks governing digital health infrastructures remain fragmented, reactive, and uneven. Applying the four-pillar framework—interoperability, cybersecurity, liability, and resilience—confirms both its analytical power and its normative urgency. While the EU offers the most comprehensive legal model, even it remains partial. Liability and resilience emerge as the weakest pillars globally, demanding urgent doctrinal innovation. These findings reinforce the central claim of this article: engineering law must evolve into a design discipline, shaping infrastructures proactively rather than merely responding to crises.

Interoperability as Legal Infrastructure

The EU experience with the European Digital COVID Certificate (EUDCC) and the European Health Data Space (EHDS) demonstrates that interoperability succeeds only when legally mandated. Binding regulations enabled rapid cross-border coordination during the pandemic. By contrast, Africa's fragmented frameworks and China's sovereignty-driven restrictions undermined system connectivity, eroding efficiency and trust. Voluntary standards and market incentives have proven inadequate. Interoperability must therefore be codified within binding instruments, ideally through the World Health Organization's revision of the International Health Regulations (IHR). Without enforceable global standards, digital health infrastructures risk collapse under the weight of fragmentation.

Cybersecurity as a Public Good

Cybersecurity obligations remain largely reactive. EUDCC vulnerabilities and weaknesses in Africa CDC platforms expose how infrastructures are only as strong as their weakest nodes. Secure-by-design principles are rarely embedded, particularly in low-capacity jurisdictions. Reliance on voluntary frameworks, such as the US NIST guidelines, perpetuates systemic fragility. Cybersecurity must be reconceptualised as a global public good, requiring binding legislation across states and private actors. The EU's NIS2 Directive provides a partial model, but international cooperation in real-time threat detection and joint incident response remains embryonic. Without universal obligations, health infrastructures remain dangerously exposed.

Liability and the Accountability Gap

Liability is the most underdeveloped pillar. Distributed infrastructures diffuse responsibility across states, private contractors, and platform operators, leaving accountability gaps that erode trust. GISAID's disclaimers of responsibility for data misuse, the diffuse attribution of fraudulent EUDCC certificates, and Africa CDC's reliance on unregulated private contractors all exemplify systemic impunity. Traditional liability doctrines cannot capture the complexity of hybrid infrastructures. Novel approaches—shared liability regimes, algorithmic accountability statutes, and no-fault compensation schemes—are required to guarantee remedies for individuals and to deter systemic neglect.

Resilience as a Legal Principle

Resilience remains rhetorical rather than operational. Although the EU and Africa CDC displayed institutional adaptability during crises, technological resilience is undermined by dependence on external vendors, political discretion, and weak legal safeguards. To sustain digital health infrastructures through pandemics, cyberattacks, and geopolitical shocks, resilience must be codified as a legal duty. Binding obligations for continuity planning, redundancy, and adaptive governance are essential, supported by funding and capacity-building for low- and middle-income countries. Without legalised resilience, infrastructures will continue to fracture under stress, perpetuating inequities.

Towards a Global Legal-Informatics Order

Fragmented regional approaches—EU rights-based regulation, US sectoral patchworks, and China's sovereignty-first model—risk entrenching a splintered digital health order. Harmonisation is imperative. Embedding the four-pillar framework within a revised IHR, aligning with emerging international cybersecurity instruments, and fostering cross-recognition of regional infrastructures would lay the foundation for a global legal-informatics commons. This shift reframes law as constitutive infrastructure, embedding equity, accountability, and resilience into the digital foundations of health governance.

RECOMMENDATIONS

Building on these insights, the following recommendations are advanced for policymakers, regulators, and scholars:

Interoperability as a Legal Imperative

Interoperability is not a technical luxury but the lifeblood of modern digital health governance. Health systems are now interdependent, reliant on cross-border data exchange to manage pandemics, track genomic risks, and sustain public health surveillance. Yet voluntary alignment and fragmented policies continue to fracture these infrastructures, eroding efficiency and trust. The European Union's regulatory successes—through the European Digital COVID Certificate (EUDCC) and the European Health Data Space (EHDS)—prove that binding legal mandates can deliver seamless connectivity. This approach must be globalised. Regional systems should adopt enforceable standards, while the World Health Organization (WHO) must integrate minimum interoperability obligations into the International Health Regulations (IHR). Anything less entrenches fragmentation, fuels sovereignty-driven closure, and undermines global solidarity. Interoperability must be codified as a legal imperative for global health security.

Strengthening Liability Regimes

Accountability is the foundation of trust. Yet distributed infrastructures—spanning states, contractors, and private platforms—too often operate in legal grey zones where responsibility is blurred and victims are left without recourse. This is unacceptable. Legislatures must design doctrines of shared liability that assign obligations across all actors. Systemic failures should never vanish into jurisdictional gaps. At the international level, no-fault compensation mechanisms must be established to guarantee remedies for individuals harmed by infrastructural breakdowns. These frameworks are not optional reforms—they are ethical necessities. Without enforceable liability, digital health governance will remain structurally unjust and politically fragile.

Operationalising Resilience

Resilience cannot remain rhetoric. It must be institutionalised as a binding legal principle. Health infrastructures must be built with continuity planning, redundancy, and adaptive capacity as legal requirements, not policy aspirations. The stakes are especially high in low- and middle-income countries, where resource scarcity compounds vulnerability. Global funding and coordination must support these obligations to ensure resilience is universal, not a privilege of the wealthy. Codified resilience will transform fragile infrastructures into systems capable of withstanding shocks, ensuring equity in protection and confidence in governance.

Cybersecurity as a Public Good

Cybersecurity is the frontline of digital health governance. It is not a matter of private compliance but a global public good demanding binding, enforceable standards. Voluntary guidelines are inadequate in a world where health systems face relentless cyberattacks. States must legislate secure-by-design principles, drawing on the EU’s NIS2 Directive, to hardwire protection into digital infrastructures from inception. Moreover, cybersecurity cannot stop at national borders. Collective defence through international cooperation—real-time threat detection, joint incident response, and shared intelligence—is indispensable. Anything less leaves critical infrastructures exposed and public health in peril.

Closing Liability Gaps

Liability gaps are systemic cracks that compromise governance. When responsibility is scattered across multiple actors, impunity flourishes, and justice is denied. Shared liability regimes must be enacted to ensure responsibility is clearly distributed and enforceable. At the global level, no-fault compensation systems should guarantee remedies for those harmed by digital health failures, even when attribution is complex. Closing liability gaps is not a technical adjustment but a moral and legal obligation. Without it, public trust will collapse under the weight of unaccountable systems.

Towards a Global Legal-Informatics Commons

The future of global health governance requires more than fragmented reforms—it demands a paradigm shift. Digital health infrastructures must be recognised as global public goods, governed by principles of equity, accountability, and transparency. The WHO must embed the four-pillar framework—interoperability, cybersecurity, liability, and resilience—into a revised IHR, transforming it into a legal foundation for the digital age. To drive accountability and foresight, a Digital Health Law Observatory should be created to monitor compliance, share best practices, and identify emerging risks. Without such a common, governance will lag fatally behind innovation.

This is the call to action: law must no longer trail technology—it must constitute its foundation. By embedding enforceable standards of interoperability, accountability, resilience, and cybersecurity, the international community can ensure that digital health infrastructures serve as resilient, just, and trustworthy pillars of global health governance. Anything less is failure by design.

CONCLUSION

This article has shown that digital health infrastructures—whether vaccination certification systems, cross-border health platforms, or genomic surveillance networks—can no longer be governed by fragmented, reactive, or sovereignty-driven legal regimes. The comparative analysis across the EU, Africa, and global genomic systems, measured against the regulatory orientations of the EU, United States, and China, exposes a fundamental weakness: existing frameworks are inadequate to deliver accountability, security, or trust in infrastructures that are now central to global health governance.

To remedy this, the article advances a four-pillar framework of interoperability, cybersecurity, liability, and resilience, not as optional reform but as a paradigm shift in law's role. Interoperability must be legally mandated to overcome fragmentation; cybersecurity must be embedded as a secure-by-design obligation; liability must be extended to close systemic accountability gaps; and resilience must be elevated into binding legal principle rather than rhetorical aspiration. Without this structural recalibration, digital health infrastructures will remain precarious, uneven, and inequitable.

The argument crystallises engineering law as an emergent discipline—redefining law not as an external regulator arriving after the fact, but as a constitutive infrastructure shaping socio-technical systems ex ante. In practice, the analysis highlights the EU's relative strength in its rights-based approach, the United States' vulnerability through fragmentation, Africa's dependence on external infrastructures, and China's sovereignty-centric closure. Collectively, these trajectories illustrate the unsustainability of the current patchwork of governance.

The COVID-19 pandemic underscored the indispensability of digital infrastructures to public health while simultaneously exposing the consequences of weak legal design: insecurity, fragmentation, and declining public trust. The four-pillar framework advanced here offers a blueprint for addressing these failures. More fundamentally, it demands that law evolve beyond its traditional reactive posture to operate as an engineered foundation of digital health governance.

The conclusion is unequivocal: engineering law is not a theoretical aspiration but an urgent necessity. Only by embedding interoperability, cybersecurity, liability, and resilience into binding legal frameworks can digital health infrastructures become resilient, accountable, and equitable. Anything less will perpetuate governance failures that undermine both health security and global justice.