ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

BRIDGING THE GAP BETWEEN U.S. HEALTHCARE SUPPLY-CHAIN CYBERSECURITY POLICY AND PRACTICE THROUGH AI-DRIVEN COMPLIANCE TOOLS

Kwadwo Adu Agyemang[1], Barbara Aryeley Aryee[2], Mariatu Mahmoud[3]
[1] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*
[2] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*
[3] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*

Article DOI: https://doi.org/10.36713/epra25510
DOI No: 10.36713/epra25510

ABSTRACT
The U.S. healthcare supply chain is crucial for guaranteeing ongoing access to necessary medications, but because of digitisation, dispersed operations and reliance on international pharmaceutical production, it is becoming more vulnerable to cyberattacks. The supply of medications is threatened, data integrity is compromised and public health risks are increased by disruptions brought on by cyberattacks, operational inefficiencies and complicated regulations. This study looks into how cybersecurity policy and practice in the US healthcare supply chain can be improved using AI-driven compliance solutions. This study employs a literature review approach to investigate supply-chain challenges and evaluate the impact of cutting-edge technologies such as blockchain, artificial intelligence, machine learning, and predictive analytics for efficient cybersecurity compliance. The findings of the study show that AI-enabled tools greatly improve operational resilience and regulatory compliance by enhancing real-time monitoring, predictive forecasting, anomaly detection and safe data sharing. Also, decentralised decision-making, tamper-proof record-keeping and traceability are further supported by blockchain and edge computing. The study therefore concludes that incorporating AI-driven compliance solutions improves cybersecurity resilience, guarantees continuous access to necessary medications and lowers the risk of supply-chain disruptions.

KEYWORDS: *Healthcare Supply Chain Cybersecurity, AI-Driven Compliance Tools, Essential Medicines, Supply Chain Vulnerabilities, Pharmaceutical Cybersecurity, Policy-Practice Gap*

INTRODUCTION
Essential medications are defined by the World Health Organisation (WHO) as drugs that address a population's top healthcare needs. In the United States, the FDA expands this idea through its list of necessary medications, medical countermeasures, and vital components important to public health emergencies and national security goals [1]. Strong cybersecurity measures, in addition to effective supply-chain operations, are necessary to ensure the ongoing availability of these items. Cyber vulnerabilities in the healthcare supply chain have the potential to degrade national preparedness, interfere with access to necessary medications, and compromise data integrity. Global disruptions in the supply of medications have been increasing, as recent WHO studies demonstrate that the effects of these disruptions exacerbate already-existing disparities and jeopardise patient safety [2]. Shukar et al. also pointed out that prescription shortages cost U.S. hospitals at least $359 million in labour expenses each year [3]. This problem is exacerbated when cyber attacks disrupt inventory, transportation, or procurement systems. These facts show that cybersecurity is now a fundamental necessity for supply-chain stability rather than a side challenge.

Data-driven technologies are becoming essential to bolstering supply-chain cybersecurity and compliance in light of these dangers. Blockchain, machine learning, and artificial intelligence (AI) technologies provide new ways to evaluate risks, identify irregularities, and automate compliance with changing cybersecurity regulations [4]. Organisations can anticipate risks, spot odd system behaviours, and detect compliance gaps before they cause disruptions with the aid of AI-powered monitoring. As healthcare organisations handle vast and varied datasets from manufacturers, distributors, and hospital networks, predictive analytics can enhance visibility across interconnected supply-chain systems. Additionally, blockchain reduces the possibility of cyber manipulation and counterfeit infiltration within supply chains by supporting tamper-proof transaction records and secure traceability [5].

These methods are quite valuable. AI-driven solutions could save the healthcare sector up to $10 billion a year through improved operational accuracy and risk mitigation, according to a 2021 Accenture report [6]. Fox et al. have indicated that better forecasting and visibility cut medication shortages by up to 30% [7]. However, putting AI-supported cybersecurity compliance technologies into practice is not simple. Healthcare systems must overcome obstacles to privacy concerns, interoperability, data quality, and regulatory limitations. Furthermore, coordinated efforts across technological, regulatory, and organisational domains are necessary to integrate AI technologies with current cybersecurity frameworks, such as NIST standards, FDA cybersecurity recommendations, and HIPAA regulations [8].

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Healthcare supply-chain challenges, cybersecurity flaws, or data-driven technologies are frequently examined separately in current literature. Nevertheless, there is little research that combines these elements into a cohesive framework that can close the growing gap between cybersecurity policy and practical application. To bridge this gap, this study suggests an AI-driven strategy for enhancing cybersecurity compliance in the U.S. healthcare supply chain, with a particular emphasis on necessary medications. In particular, the study seeks to:

- Determine the main cybersecurity challenges and compliance roadblocks impacting the U.S. healthcare supply chain for necessary medications.
- Analyse how AI-driven tools, such as blockchain, automated monitoring, real-time anomaly detection, and predictive analytics, can support and expedite cybersecurity compliance.
- Examine real-world examples where these technologies have been successfully implemented and draw lessons for wider adoption.
- Make recommendations for strategic initiatives and policies that help expedite the use of AI-enabled compliance tools while resolving interoperability, workforce, and regulatory obstacles.

Through the efficient integration of AI-driven compliance technology, the main objective is to provide a workable roadmap that assists healthcare stakeholders in enhancing cybersecurity resilience, guaranteeing regulatory alignment, and safeguarding continuous access to necessary medications.

2. LITERATURE REVIEW

2.1 Supply-Chain Challenges Contributing to the Cybersecurity Policy–Practice Gap

The efficiency and security of the U.S. healthcare supply chain are threatened by a number of operational and structural issues. The lack of transparency among producers, distributors, and healthcare providers is a recurring problem. Coordinated responses to disruptions are challenging because stakeholders frequently work in isolated information environments, which leads to uneven and non-standard data sharing [9]. Because visibility is crucial for tracking system integrity and identifying anomalies, these disjointed communication channels not only impede decision-making but also make it more difficult to put strong cybersecurity procedures into place.

The nation's heavy reliance on foreign production of necessary pharmaceutical components is another significant challenge. The development of generic drugs in the United States is largely dependent on active pharmaceutical ingredients (APIs), which are mostly derived from China and India, which together provide around 80% of the APIs used domestically [1]. About 40% of generic medications imported into the United States come from India alone, while China continues to be the biggest provider of essential raw ingredients and APIs [10]. Significant vulnerability to regional shutdowns or geopolitical tensions is introduced by this concentration of output. China's plant shutdown during the COVID-19 epidemic exposed the vulnerability of this reliance by upsetting international pharmaceutical supply systems [12]. Because strained systems depended on quick digital coordination under extreme pressure, these breakdowns also enhanced potential for cyber attack.

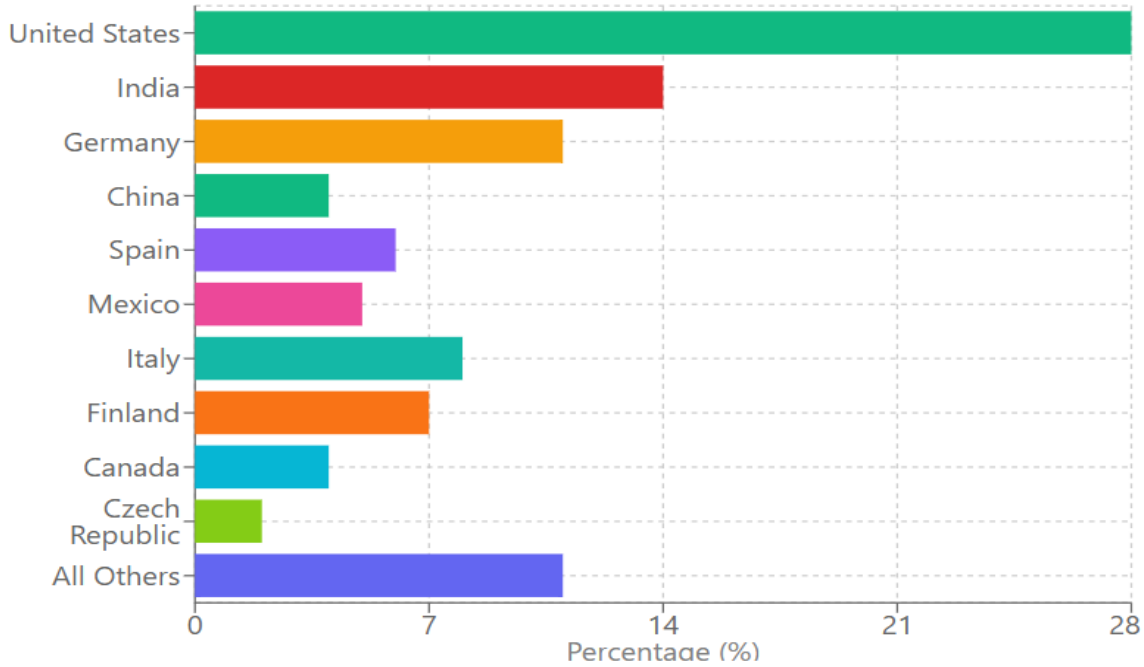
Supply-chain resilience is further complicated by inventory management procedures. Although just-in-time inventory systems lower storage costs during regular business operations, they do not provide much of a buffer in the event of demand spikes or disruptions [13]. Early in the COVID-19 pandemic, this strategy led to significant shortages of numerous necessary medications and personal protective equipment (PPE) [14]. Inventory systems are becoming more reliant on safe data flows as they become more digitalised, which means that cyber vulnerabilities can easily result in operational shortages.

Additional challenges come from regulatory complexity. Timely reactions to shortages and operational problems may be delayed by protracted approval procedures for new suppliers, manufacturing modifications, or production scale-ups [15]. Decisions on sourcing and distribution are further complicated by variations in international regulatory requirements. When cybersecurity compliance requirements are added, these regulatory layers become even more difficult to apply consistently for many organisations because of a lack of resources, inconsistent interpretations, and disjointed oversight.

Lastly, cybersecurity risks continue to pose a danger to the healthcare supply chain. New vulnerabilities are introduced as supply-chain processes grow increasingly digital, incorporating cloud-based platforms, electronic procurement systems, and automated logistics [16]. Cyberattacks could stop production, tamper with inventory information, interfere with distribution or compromise private patient and product data. A coordinated, data-driven approach that can coordinate supply-chain operations, cybersecurity regulations, and new AI-driven compliance technologies is necessary to address these complex issues and create a more robust national infrastructure.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Figure 1: Manufacturing Facility Locations for Drugs in Shortage (2023)



Source: U.S. Food and Drug Administration (FDA). (2023).

With only 28% of these facilities situated domestically in the United States, the geographic distribution of pharmaceutical production facilities that face shortages in 2023 exposes serious supply chain vulnerabilities. A complicated multinational reliance structure results from the fact that 25% of shortage-prone manufacturing capacity is shared by Germany and India, with the remainder facilities spread across nine other nations. Due to the dispersed global production footprint, there are several points of failure where domestic medicine shortages could result from regional disruptions, geopolitical tensions, or cyberattacks. Both physical supply chain risks and digital vulnerabilities across interconnected procurement, logistics, and inventory management systems are increased by the concentration of vital pharmaceutical production in foreign jurisdictions, especially those with disparate cybersecurity standards and regulatory frameworks.

2.2. Essential Medicines and Cybersecurity Implications in the U.S. Healthcare Supply Chain

The idea of essential medications is central to the formulation and execution of global health strategy. Essential medications are those that address a population's top healthcare needs, according to the World Health Organisation (WHO) [2]. Clinical efficacy, safety, cost-effectiveness, and public health importance are taken into consideration while making selections. The WHO Model List of Essential Medicines, which was first published in 1977 and is updated every two years, has influenced healthcare planning and policy all across the world and has been used as a global reference point for national essential medicine lists [17].

To meet the unique clinical and national security requirements of the United States, the Food and Drug Administration (FDA) modified this framework. In response to supply-chain fragility issues and vulnerabilities discovered during the COVID-19 pandemic, the FDA published a list of key medications and crucial inputs in 2020 [1]. This list emphasises the drugs and supplies required for efficient patient treatment as well as for preserving operational preparedness in the event of pandemics, natural catastrophes, and biosecurity risks. Strong cybersecurity measures are also necessary to preserve the availability of these vital medications and guarantee the integrity of procurement and distribution systems as the healthcare supply chain becomes more digitalised.

Beyond their clinical uses, vital drugs are important. A health system's ability, resiliency, and readiness are indicated by its constant availability [18]. Emergency response, primary healthcare services, and the management of chronic diseases are all supported by reliable access. Disruptions have immediate and serious effects on public health, whether they are brought on by supply-chain limitations, cyberattacks, or manufacturing failures. The cybersecurity aspect is becoming more and more important because the continuous supply of necessary medications might be directly threatened by unauthorised access, inventory data manipulation, or interruptions to automated ordering systems.

Important medications have significant financial ramifications as well. Despite making up a small percentage of the overall pharmaceutical industry, they play a crucial role in healthcare finance methods, especially in low- and middle-income nations where system viability depends on affordable therapies [19]. Essential drugs help stabilise healthcare costs and direct sensible resource allocation in high-income countries like the United States. To avoid fraud, data breaches, or operational disruptions that could raise costs or skew supply availability, the digital systems used to handle pricing, reimbursement, and procurement procedures must be secure.

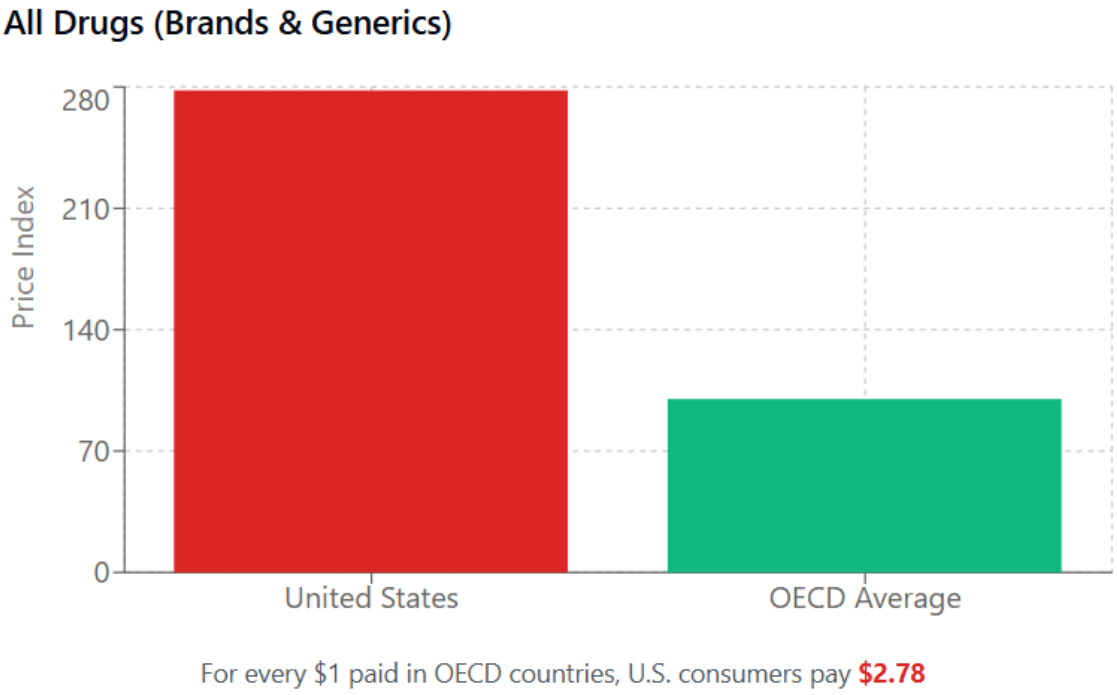
ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

From the standpoint of public health, important medications continue to play a crucial role in managing infectious diseases like HIV/AIDS, TB, and malaria, as well as chronic conditions like diabetes and cardiovascular disease [20]. Antivirals, critical care medications, and vaccinations are in high demand during global emergencies such as the COVID-19 pandemic, which makes crucial treatments even more vital [21]. Cybersecurity risks also increase during these times as malevolent actors try to alter vaccination distribution data, target overworked supply-chain systems, or take advantage of weaknesses in digital procurement networks.

In the United States, access to necessary medications is still unequal despite their significance. A considerable section of the population cannot afford many necessary treatments due to the high cost of prescription drugs, which are on average 2.56 times higher in the United States than in other high-income nations [22]. This discrepancy is exacerbated by the lack of robust price regulatory systems compared to nations that employ price ceilings or government negotiations [23]. Strong cybersecurity safeguards are also necessary for digital pricing platforms and automated claims systems used by distributors and insurers, since cyber events in these systems further impede access or raise patient expenses.

Geographical and social factors also contribute to access discrepancies. Rural hospitals are more likely to experience stockouts, longer delivery periods, and higher distribution costs. Financial obstacles and unstable supply cause low-income and uninsured patients to have their access delayed or refused [18]. The need for systemic changes is highlighted by these access issues as well as weaknesses in digital supply-chain systems. Enhancing cybersecurity compliance throughout the supply-chain infrastructure is crucial to guaranteeing consistent availability as well as safeguarding the equity, affordability, and integrity of necessary medications for all Americans.

Figure 2: U.S. Prescription Drug Prices vs. OECD Countries (2022)



Source: Office of the Assistant Secretary for Planning and Evaluation (ASPE),

According to the ASPE 2022 analysis, American consumers pay 2.78 times more for prescription drugs than the OECD average, resulting in significant financial barriers that keep millions of Americans from obtaining necessary medications for managing chronic illnesses, responding to emergencies, and preparing for pandemics. The fair distribution of the 319 essential medications that the FDA has designated as crucial for national health security is directly threatened by this pricing disparity, which is made worse by the lack of strong price regulatory mechanisms like government negotiations or price ceilings used by other high-income countries. The digital infrastructure that underpins pharmaceutical pricing, such as electronic pricing platforms, procurement networks, and automated claims processing systems, poses a serious cybersecurity risk because malevolent actors could use these systems to commit fraud, alter pricing data, or disrupt operations, all of which would worsen already-existing affordability issues. Therefore, it is crucial to use AI-driven cybersecurity compliance tools to safeguard these digital pricing and distribution systems in order to prevent cyber-induced cost inflation as well as to protect the integrity, availability, and equitable access to essential medicines for all Americans, especially vulnerable populations in underserved and rural communities.

3. DATA-DRIVEN STRATEGIES FOR STRENGTHENING CYBERSECURE SUPPLY CHAIN RESILIENCE

In light of the growing intersections between operational weaknesses and cyber threats, this section explores how

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

cutting-edge data analytics and emerging technologies can modernise and safeguard the U.S. healthcare supply chain. The healthcare system needs technologies that boost cybersecurity compliance while simultaneously increasing efficiency in a climate marked by geopolitical uncertainty, natural disasters and increasing digital risk. By combining real-time data systems, predictive algorithms and AI-driven compliance solutions, organizations can improve visibility, identify irregularities early, and create flexible procedures that safeguard vital medications from both physical disturbances and cyberattacks. The useful frameworks and technologies that facilitate risk foresight, quick response, and safe operational continuity are described in the next subsections.

3.1 Big Data Analytics for Cybersecurity Monitoring and Operational Visibility

Modernising and safeguarding healthcare supply-chain operations heavily relies on big data analytics. Organisations can obtain a thorough understanding of supply-chain behaviour by combining several data sources, such as pharmacy sales data, inventory and logistics information, electronic health records (EHRs), and publicly accessible digital platforms. Both operational planning and the detection of cyber abnormalities, including unauthorised system access or altered inventory data, depend on this integrated view. Big data analysis has been shown by Moons et al. to be more than 80% accurate in predicting medicine shortages up to 12 months ahead of time [24]. When paired with cybersecurity monitoring, this predictive strength becomes even more beneficial, allowing for automated notifications when data abnormalities indicate possible intrusions. Evidence from Uthayakumar and Priyan also shows that big-data-enhanced inventory systems can reduce costs by 30% while improving service continuity for pharmaceuticals [25], showing the dual operational and cybersecurity benefits of smarter data ecosystems.

3.2 Artificial Intelligence (AI) and Machine Learning (ML) for Compliance Enforcement

By identifying complex patterns and producing forecasting insights that are beyond human capabilities, artificial intelligence (AI) and machine learning improve supply-chain resilience. When these technologies are modified for cybersecurity compliance, they become particularly potent. AI systems are able to continuously analyse digital supply-chain settings, spot anomalous data flows, and instantly identify malware or unauthorised transactions. AI helps with route optimisation, demand forecasting, and disruption prediction in physical logistics. In inventory management, reinforcement learning systems have demonstrated significant benefits. These algorithms, according to Oroojlooyjadid et al., perform better than traditional inventory tactics by lowering the likelihood of both stockouts and overstock situations for necessary medications [26]. AI-driven compliance technologies automatically confirm data integrity, identify any tampering, and guarantee that digital exchanges throughout the supply chain adhere to legal standards when combined with cybersecurity frameworks.

3.3 Predictive Modelling for Secure Demand Forecasting

A crucial part of supply-chain planning is predictive modelling, which provides more accurate demand forecasting for all necessary drugs. To accurately predict future demands more, these models examine past sales, disease patterns, demographic shifts, and economic variables. When compared to traditional time-series methods, Yani et al. showed that machine learning models increase forecasting accuracy by 15 to 20% [27]. Predictive modelling has an additional function in a cybersecurity-enhanced framework, as it detects unanticipated deviations in predicting patterns caused by data corruption or cyber intrusion. Healthcare organizations can identify discrepancies, verify data integrity, and make sure that fraudulent activity does not skew demand signals by combining predictive analytics with AI-driven compliance systems.

3.4 Real-Time Inventory Management for Cyber-Resilient Operations

Real-time inventory systems offer constant visibility into stock levels throughout the healthcare supply chain. They are powered by IoT devices, RFID tags, smart sensors, and cloud-based platforms. When demand suddenly changes, these systems facilitate quick redistribution and automated resupply. A study by Thapa et al. found that real-time inventory management can reduce expired medicines by 54% and stock-outs by 25% [28]. These systems also serve as front-line defence mechanisms when combined with cybersecurity measures, allowing for the quick detection and containment of unauthorised access attempts, anomalous sensor readings, or manipulated inventory files. Even as cyber threats become more sophisticated, secure real-time systems help guarantee that automated ordering and distribution procedures continue to be reliable.

3.5 Blockchain Technology for Transparency and Tamper-Proof Compliance

Blockchain provides a powerful way to improve pharmaceutical supply chains' cyber resistance, traceability, and transparency. Blockchain records offer tamper-resistant audit trails that are extremely beneficial for regulatory compliance since they are decentralised, unchangeable, and verifiable. Blockchain facilitates safe recall management, real-time supply chain tracing, and drug product authentication. By guaranteeing end-to-end visibility from producers to dispensers, blockchain can effectively meet Drug Supply Chain Security Act (DSCSA) standards, as proved by the Chronicled and LinkLab test in 2019 [29]. Blockchain-based compliance solutions will not only lessen the possibility of fake medications, but they also help stop fraudulent transactions, unauthorised system modifications, and data manipulation in all major weaknesses in legacy digital systems.

3.6 Advanced Risk Analytics for Cybersecurity-Driven Decision Making

Healthcare organisations can find weaknesses in both physical and digital supply-chain networks due to advanced risk analytics. These instruments measure the financial health of important partners, track geopolitical upheavals, estimate natural disaster risks, and evaluate supplier dependability. Tucker et al. demonstrated that network analysis methods pinpoint the pharmaceutical supply chain's weak points and crucial nodes, offering practical guidance for enhancing resilience [30]. Risk analytics can also identify digital vulnerabilities, give high-risk asset protection top priority, and

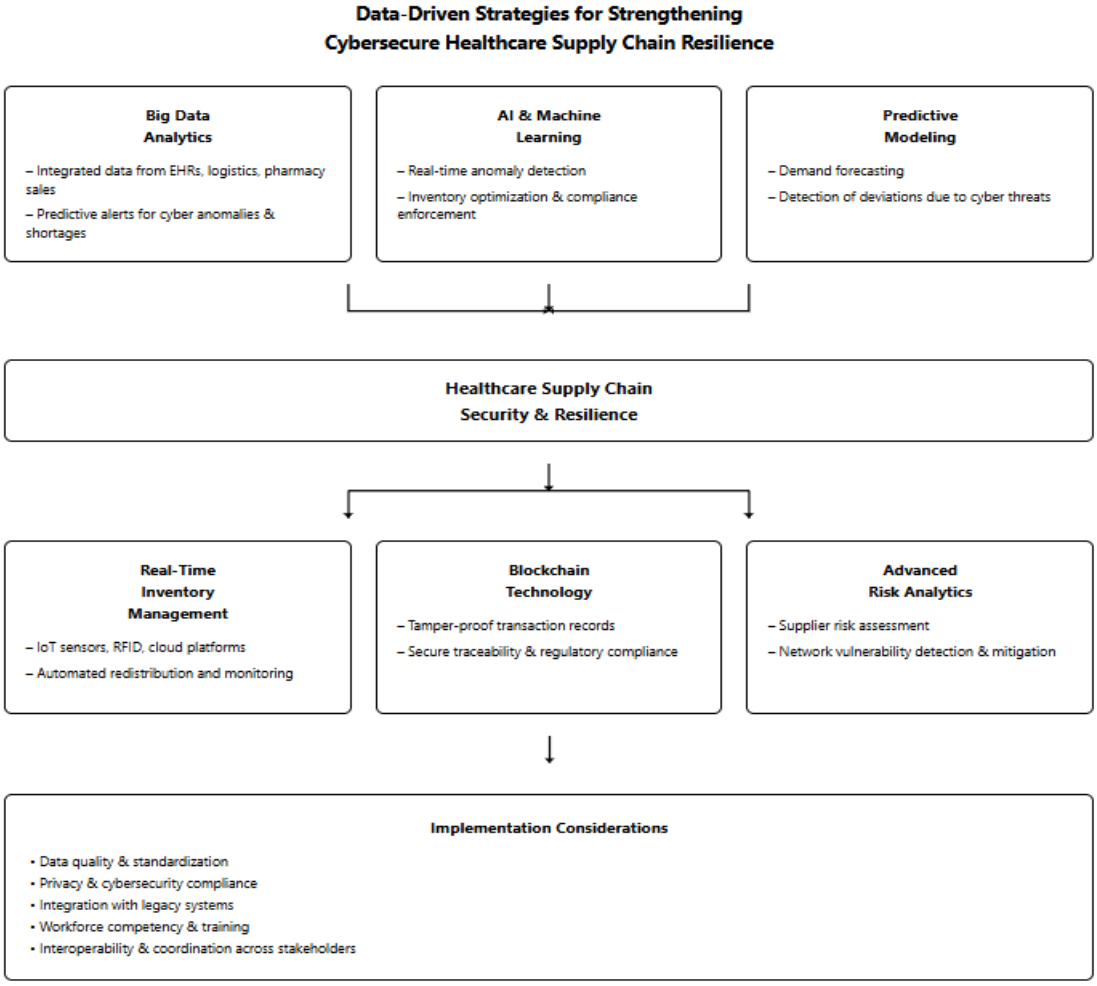
ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

automate compliance reporting when integrated into cybersecurity policy frameworks. The financial and security benefits of using AI-driven compliance solutions are significant, with estimates indicating that AI adoption in healthcare operations saves between 5 and 10% of overall spending, or $200 billion to $360 billion yearly [31].

3.7 Implementation Considerations for AI-Driven Compliance Tools

Implementing these data-driven initiatives necessitates resolving issues, including data quality, interoperability, privacy, and coordination among various supply-chain partners, notwithstanding their disruptive potential. To properly use AI-driven solutions, digital systems must conform to cybersecurity regulations and federal policy. Healthcare organizations may secure necessary medications, avoid operational disruptions, and close the gap between policy recommendations and everyday practice by combining blockchain, real-time monitoring, and predictive analytics with AI compliance solutions.

Figure 3: Integrated Data-Driven Framework for Enhancing Cybersecurity and Resilience in the U.S. Healthcare Supply Chain



The figure above displays a cohesive framework showing how data-driven technologies increase cybersecurity and resilience within the U.S. healthcare supply chain. Big data analytics, artificial intelligence, machine learning, and predictive modelling are the main analytical skills highlighted at the top. These skills contribute to better anomaly detection, compliance enforcement, demand forecasting, and early alerts of cyber-related disturbances. Together, these skills improve the security and resilience of the healthcare supply chain as a whole. Three operational enablers are presented in the middle section: enhanced risk analytics, blockchain technology, and real-time inventory management. These components facilitate supplier risk assessment, automated monitoring, secure traceability, and network vulnerability reduction. Key implementation factors, including data standardisation, cybersecurity and privacy standards, legacy system integration, workforce training, and cross-stakeholder collaboration, are outlined at the bottom of the diagram. When combined, the elements demonstrate how a more robust, cyber-secure healthcare supply chain is created by fusing powerful analytics with transparent, safe technologies.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

4. CHALLENGES IN IMPLEMENTING AI-DRIVEN CYBERSECURITY COMPLIANCE TOOLS IN THE U.S. HEALTHCARE SUPPLY CHAIN

Although AI-driven and data-centric approaches have enormous promise to improve healthcare supply chains' operational effectiveness and cybersecurity, there are several structural, technological, and legal obstacles to their adoption. To ensure continuous access to necessary medications while protecting sensitive data, these issues must be carefully addressed to close the gap between cybersecurity policy requirements and practical application.

4.1 Ensuring Data Quality and Standardization Across the Supply Chain

When using AI-driven compliance technologies, data quality and standardisation continue to be fundamental obstacles. Electronic health records (EHRs), pharmacy sales systems, inventory logs, IoT-enabled sensors, and logistics platforms are just a few of the diverse sources from which healthcare supply chains create data. Predictive analytics and AI-driven risk assessments may be jeopardised by these data streams' frequent variations in format, completeness, and dependability. Inaccurate demand forecasting, incorrect cyber threat assessment, and faulty compliance reporting can all result from poor data quality. It is crucial to standardise data collection techniques and develop unified data schemas for all supply-chain actors, but doing so takes a lot of time, money, and stakeholder coordination. Even the most sophisticated AI systems are unable to precisely monitor cybersecurity compliance or operational performance in the absence of a dependable standardised data infrastructure [32].

4.2 Privacy and Cybersecurity Compliance Challenges

AI-driven supply-chain systems must adhere to cybersecurity best practices and operate within stringent regulatory frameworks, such as HIPAA in the United States. There are two challenges in protecting sensitive patient data while allowing manufacturers, distributors, and healthcare providers to share data. Operational disruption and harsh regulatory penalties may follow any data breach or misuse. It is especially difficult to ensure security and privacy when integrating AI systems that examine pooled datasets from several organisations. AI-driven compliance solutions must also constantly adjust to new vulnerabilities, such as ransomware attacks, unauthorised system access, and data modification, without going against privacy rules due to the dynamic nature of cyber threats [33].

4.3 Integration with Legacy Systems and Digital Infrastructure

The widespread use of legacy IT infrastructure in healthcare organisations is a major obstacle to the implementation of AI-driven compliance tools. ERP, EHR, and inventory management systems that are not intrinsically compatible with cutting-edge AI analytics, blockchain solutions, or real-time monitoring platforms are nonetheless widely used by hospitals, pharmacies, and distributors. Complex middleware, data migration, and customisation are necessary for integrating AI tools with these legacy systems, frequently at significant operational and financial costs [34]. Adoption may be slowed, cybersecurity monitoring may have blind spots, and the overall effectiveness of AI-driven compliance frameworks may be diminished by incompatible systems.

4.4 Workforce Competency and Change Management

Skilled workers who can understand data analytics, update AI models, and react to cybersecurity alarms are essential for the successful deployment of AI-driven compliance technologies. However, there is a severe lack of individuals with simultaneous training in supply-chain management, cybersecurity, and artificial intelligence in the healthcare industry [35]. To give supply-chain employees, IT professionals, and compliance officials the skills they need to use AI solutions efficiently, training programs must be created. Change management is also essential since opposition to new procedures or technologies can impede adoption and lower the effectiveness of compliance. To successfully close the policy-practice gap, organisations must cultivate a culture that prioritises ongoing education and cybersecurity awareness.

4.5 Navigating Evolving Regulatory Compliance and Policy Ambiguity

Healthcare supply chains subjected to strict regulations and frameworks for compliance are always changing, especially in reaction to new cybersecurity risks. AI-driven tool implementation frequently necessitates balancing new capabilities with current legal and regulatory requirements, such as FDA guidelines, HIPAA rules, and the Drug Supply Chain Security Act (DSCSA). Adoption may be hampered by uncertainty over cross-border data management, auditing requirements, and liability. As a result, AI systems must be made to offer visible, auditable procedures that meet present legal requirements while being flexible enough to accommodate future policy modifications [36].

4.6 Achieving Interoperability Across Complex Healthcare Networks

Smooth data sharing between many stakeholders, such as manufacturers, distributors, hospitals, pharmacies, and regulatory bodies, is essential to effective AI-driven cybersecurity compliance. Data standards, proprietary software, and disparities in technological platforms all contribute to interoperability issues. Interoperability issues can lead to operational inefficiencies, blind spots in cybersecurity monitoring, and delayed identification of cyber attacks or supply-chain disruptions [37]. Overcoming these obstacles requires creating industry-wide standards, implementing standardised APIs, and utilising safe data-sharing frameworks.

4.7 Financial and Organizational Constraints

It takes a significant investment in technology, cybersecurity infrastructure, and personnel development to implement AI-driven compliance tools. Disparities in supply-chain resilience and cybersecurity readiness may worsen in smaller hospitals, rural providers, and community pharmacies due to financial and technical limitations. These expenses can be mitigated by public-private partnerships, government incentives, and strategic alliances, but organizations must carefully consider how resource constraints may affect operational integrity and compliance.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

5. POLICY RECOMMENDATIONS AND FUTURE DIRECTIONS FOR AI-DRIVEN CYBERSECURE HEALTHCARE SUPPLY CHAINS

When implementing targeted policy actions, encouraging stakeholder collaboration, investing in technology infrastructure, and building a workforce capable of handling both operational and cybersecurity demands are all necessary to fully utilise AI-driven tools for bridging the gap between cybersecurity policy and practice in the U.S. healthcare supply chain. These strategies are vital for guaranteeing safe, reliable, and continuous access to necessary medications.

5.1 Policy Recommendations

For AI-driven cybersecurity compliance to be effective, industry-wide standards must be established. Hospitals, distributors, manufacturers, and regulatory agencies can all benefit from increased use of HL7's FHIR (Fast Healthcare Interoperability Resources) platform [38]. AI compliance technologies may be seamlessly integrated with standardised data, enabling automated cybersecurity adherence monitoring, anomaly detection, and audit reporting. For these criteria to be widely adopted and consistently enforced, coordination between the FDA, ONC, GS1, and private healthcare organisations is crucial.

In order to allow the integration of AI, blockchain, and IoT in healthcare supply chains while maintaining cybersecurity and operational compliance, current policies must change. Advanced digital solutions that can enhance traceability, integrity, and compliance monitoring should be included in the FDA's Drug Supply Chain Security Act (DSCSA). To avoid abuse or unforeseen repercussions, ethical standards for the use of AI, such as algorithm responsibility, explainability and transparency must be legislated. Rapid, secure responses to supply disruptions can also be made possible by streamlining regulatory approval for new suppliers or production procedures during public health emergencies.

When testing and scaling AI-driven compliance solutions, government agencies, healthcare providers, and tech businesses must collaborate [39]. A model for wider adoption should be provided by pilot projects like supply-chain tracing enabled by blockchain under the DSCSA. To ensure adherence to cybersecurity regulations while preserving operational effectiveness, the HHS, FDA, pharmaceutical makers, and distributors should work together to develop a common framework for secure AI deployment.

Healthcare organizations need assistance in modernizing their outdated IT systems to incorporate cloud-based analytics, real-time inventory platforms, and AI-driven compliance tools [40]. Grants, tax credits, and cost-sharing arrangements are examples of federal and state incentives that might lessen the cost of modernisation. By facilitating automated monitoring, anomaly detection, and regulatory reporting, modern infrastructure will not only improve operational efficiency but also fortify cybersecurity resilience.

A workforce with expertise in supply-chain management, cybersecurity, and artificial intelligence is necessary to close the policy-practice gap. It is essential to build professional development pathways, degree programs, and specialised certifications in healthcare supply-chain analytics and AI-driven compliance. Professionals will be prepared to manage intricate, digitally connected supply chains that adhere to changing cybersecurity regulations through cooperation between federal agencies, industry associations like ASCM, academic institutions, and healthcare employers.

CONCLUSION

To guarantee continuous access to necessary medications, it is imperative to close the gap between U.S. healthcare supply-chain cybersecurity policy and practice. This study shows how AI-driven compliance technologies backed by blockchain, edge computing, real-time monitoring, and predictive analytics provide effective ways to match operational procedures with changing legal requirements. Strategic investments in technology, infrastructure, policy revisions, and professional training can help overcome obstacles like data quality, interoperability, legacy system integration, and workforce capacity. Healthcare organizations can create robust, safe, and flexible supply chains by promoting public-private cooperation, standardizing data and compliance procedures, and integrating cutting-edge cybersecurity frameworks. In the end, incorporating AI-driven compliance solutions improves cybersecurity resilience and protects public health, lowers operational inefficiencies, and guarantees fair, dependable access to necessary medications in the face of operational and digital disruptions.

REFERENCES

1. *Guharoy, R., & Noviasky, J. (2021, July). Executive Order on Ensuring Essential Medicines–All Bark, No Bite?. In Mayo Clinic Proceedings (Vol. 96, No. 7, pp. 1714-1717). Elsevier.*
2. *World Health Organization. (2023). The selection and use of essential medicines 2023: web annex A: World Health Organization model list of essential medicines: 23rd list (2023) (No. WHO/MHP/HPS/EML/2023.02). World Health Organization.*
3. *Shukar, S., Zahoor, F., Hayat, K., Saeed, A., Gillani, A. H., Omer, S., ... & Yang, C. (2021). Drug shortage: causes, impact, and mitigation strategies. Frontiers in pharmacology, 12, 693426.*
4. *Srinivasan, R., & Swink, M. (2018). An investigation of visibility and flexibility as complements to supply chain analytics: An organizational information processing theory perspective. Production and Operations Management, 27(10), 1849-1867.*
5. *Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An exploration of challenges and opportunities in the health supply chain. Blockchain in healthcare today.*
6. *Dada, S. A., Azai, J. S., Umoren, J., Utomi, E., & Akonor, B. G. (2025). Strengthening US healthcare Supply Chain Resilience Through Data-Driven Strategies to Ensure Consistent Access to Essential Medicines. Strengthening US healthcare Supply Chain Resilience Through Data-Driven Strategies to Ensure Consistent Access to Essential Medicines, 164(1), 10-10.*
7. *Fox, E. R., Sweet, B. V., & Jensen, V. (2014, March). Drug shortages: a complex health care crisis. In Mayo Clinic Proceedings (Vol. 89, No. 3, pp. 361-373). Elsevier.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

8. *Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.*
9. *Dai, T., Bai, G., & Anderson, G. F. (2020). PPE supply chain needs data transparency and stress testing. Journal of general internal medicine, 35(9), 2748-2749.*
10. *Lodh, R., & Dey, O. (2023). Trade Implications on Active Pharmaceutical Ingredients (APIS) Due to COVID-19 Pandemic and India China Altercation. The Journal of Developing Areas, 57(4), 155-174.*
11. *Mullin, R. (2020). COVID-19 is reshaping the pharmaceutical supply chain. Chemical & Engineering News, 98(16).*
12. *Handfield, R., Finkenstadt, D. J., Schneller, E. S., Godfrey, A. B., & Guinto, P. (2020). A commons for a supply chain in the post-COVID-19 era: the case for a reformed strategic national stockpile. The Milbank Quarterly, 98(4), 1058-1090.*
13. *Durugbo, C. M., & Al-Balushi, Z. (2023). Supply chain management in times of crisis: a systematic review. Management Review Quarterly, 73(3), 1179-1235.*
14. *Patel, A., D'Alessandro, M. M., Ireland, K. J., Burel, W. G., Wencil, E. B., & Rasmussen, S. A. (2017). Personal protective equipment supply chain: lessons learned from recent public health emergency responses. Health security, 15(3), 244-252.*
15. *Woodcock, J., & Wosinska, M. (2013). Economic and technological drivers of generic sterile injectable drug shortages. Clinical Pharmacology & Therapeutics, 93(2), 170-176.*
16. *Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. Health Economics and Management Review, 4(4), 17-27.*
17. *Wirtz, V. J., Hogerzeil, H. V., Gray, A. L., Bigdeli, M., de Joncheere, C. P., Ewen, M. A., ... & Reich, M. R. (2017). Essential medicines for universal health coverage. The Lancet, 389(10067), 403-476.*
18. *Persaud, N., Jiang, M., Shaikh, R., Bali, A., Oronsaye, E., Woods, H., ... & Heneghan, C. (2019). Comparison of essential medicines lists in 137 countries. Bulletin of the World Health Organization, 97(6), 394.*
19. *Beran, D., Ewen, M., & Laing, R. (2016). Constraints and challenges in access to insulin: a global perspective. The lancet Diabetes & endocrinology, 4(3), 275-285.*
20. *Bigdeli, M., Jacobs, B., Tomson, G., Laing, R., Ghaffar, A., Dujardin, B., & Van Damme, W. (2013). Access to medicines from a health system perspective. Health policy and planning, 28(7), 692-704.*
21. *Iyengar, S., Hedman, L., Forte, G., & Hill, S. (2016). Medicine shortages: a commentary on causes and mitigation strategies. BMC medicine, 14(1), 124.*
22. *Bosworth, A., Sheingold, S., Finegold, K., De Lew, N., & Sommers, B. D. (2022). Price increases for prescription drugs, 2016–2022. Office of the Assistant Secretary for Planning and Evaluation: Washington, DC, USA.*
23. *Kesselheim, A. S., Avorn, J., & Sarpatwari, A. (2016). The high cost of prescription drugs in the United States: origins and prospects for reform. Jama, 316(8), 858-871.*
24. *Moons, K., Waeyenbergh, G., & Pintelon, L. (2019). Measuring the logistics performance of internal hospital supply chains–a literature study. Omega, 82, 205-217.*
25. *Uthayakumar, R., & Priyan, S. (2013). Pharmaceutical supply chain and inventory management strategies: Optimization for a pharmaceutical company and a hospital. Operations Research for Health Care, 2(3), 52-64.*
26. *Oroojlooyjadid, A., Snyder, L. V., & Takáč, M. (2020). Applying deep learning to the newsvendor problem. Iise Transactions, 52(4), 444-463.*
27. *Yani, L. P. E., & Aamer, A. (2023). Demand forecasting accuracy in the pharmaceutical supply chain: a machine learning approach. International journal of pharmaceutical and healthcare marketing, 17(1), 1-23.*
28. *Thapa, K., & Poudel, M. (2023). AI-Based Forecasting Models for Inventory and Supply Chain Optimization in Healthcare Facility Management. International Review of Experimental Sciences, Scientific Discoveries, and Technological Advancements, 7(10), 1-12.*
29. *Naresh, V. S., Sada, R., Allu, R. J. P., Gubbala, A. D., & Bandaru, U. D. (2025). Exploring the potential of blockchain technology in modern healthcare systems. Peer-to-Peer Networking and Applications, 18(6), 314.*
30. *Tucker, E. L., Daskin, M. S., Sweet, B. V., & Hopp, W. J. (2020). Incentivizing resilient supply chain design to prevent drug shortages: policy analysis using two-and multi-stage stochastic programs. IISE Transactions, 52(4), 394-412.*
31. *Harris, B. H., Mehrotra, N., & So, E. (2024). The Fiscal Frontier: Projecting AI's Long-term Impact on the US Fiscal Outlook. Brookings Institution.*
32. *Hasan, R., Kamal, M. M., Daowd, A., Eldabi, T., Koliousis, I., & Papadopoulos, T. (2024). Critical analysis of the impact of big data analytics on supply chain operations. Production Planning & Control, 35(1), 46-70.*
33. *Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In 2014 IEEE international congress on big data (pp. 762-765). IEEE.*
34. *Aceto, G., Persico, V., & Pescapé, A. (2018). The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications, 107, 125-154.*
35. *Fosso Wamba, S., Gunasekaran, A., Dubey, R., & Ngai, E. W. (2018). Big data analytics in operations and supply chain management. Annals of Operations Research, 270(1), 1-4.*
36. *D'souza, S., Nazareth, D., Vaz, C., & Shetty, M. (2021, May). Blockchain and AI in pharmaceutical supply chain. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).*
37. *He, J., Baxter, S. L., Xu, J., Xu, J., Zhou, X., & Zhang, K. (2019). The practical implementation of artificial intelligence technologies in medicine. Nature medicine, 25(1), 30-36.*
38. *Bender, D., & Sartipi, K. (2013, June). HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In Proceedings of the 26th IEEE international symposium on computer-based medical systems (pp. 326-331).*
39. *Ajayi-Kaffi, O. V. (2024). Is Agile methodology better than waterfall approach in enhancing effective communication in healthcare process improvement projects? International Journal of Research Publication and Reviews, 5(11), 3648–3651.*
40. *Ajayi-Kaffi, O., Emmanuel, I., Azonuche, T. I., & Ijiga, O. M. (2025). Agile-Driven Digital Transformation Frameworks for Optimizing Cloud-Based Healthcare Supply Chain Management Systems. International Journal of Scientific Research and Modern Technology, 4(5), 138–156.*