RESEARCH PAPER

DIGITAL FORENSICS IN PHARMACEUTICAL CYBERCRIME: AI-BASED INVESTIGATION OF DRUG DATA MANIPULATION

Tanu Gupta[1], Vinod Kumar[2], Radheshyam Prasad[3]

[1]Research Scholar, Amity Law School, Amity University Jaipur, Rajasthan.
[2]Associate Professor, Amity Law School, Amity University Jaipur, Rajasthan.
[3]Professor of Law (Dr.), Faculty of Law, University of Lucknow, Lucknow (U.P.), India.

***Corresponding Author: Tanu Gupta | Email: tanuguptaamity09@gmail.com | Mobile No.: +91-7800054440**

ABSTRACT

The pharmaceutical and healthcare sectors have rapidly adopted digital technologies such as Electronic Health Records (EHRs), Artificial Intelligence (AI), cloud computing, and blockchain-based supply chain systems. While these technologies have improved drug development, clinical trials, and healthcare management, they have also introduced substantial cybersecurity risks. Pharmaceutical companies are increasingly targeted for cybercrime, including data theft, ransomware, manipulation of clinical trial data, creation of counterfeit drug supply chains, and intellectual property theft. Vaccine research breaches, ransomware attacks on healthcare institutions, and pharmaceutical data falsification illustrate the growing danger of pharmaceutical cybercrime to public health and patient safety. This research explores the application of digital forensics techniques and AI-powered tools for the detection, investigation and prevention of pharmaceutical cybercrime. The study examines AI-powered anomaly detection systems, machine learning algorithms, and blockchain authentication technologies to detect fraudulent clinical trial results, fake drugs, and suspicious supply chain activities. Using doctrinal and analytical research methodology with comparative legal analysis, the results show that current legislation remains fragmented and inadequate. The study recommends a multi-faceted legal-technological approach integrating AI-based monitoring, blockchain authentication, digital forensic preparedness, mandatory cybersecurity measures, and international cooperation to secure healthcare systems in the digital era.

Keywords: Digital Forensics; Pharmaceutical Cybercrime; Artificial Intelligence; Drug Data Manipulation; Blockchain Authentication; Healthcare Cybersecurity.

How to cite this article: Gupta T, Kumar V, Prasad R. Digital Forensics in Pharmaceutical Cybercrime: AI-Based Investigation of Drug Data Manipulation. Int J Drug Deliv Technol. 2026;16(56s): 280-285. DOI: 10.25258/ijddt.16.56s.29

Source of support: Nil.

Conflict of interest: None.

1. Introduction

The pharmaceutical and healthcare industry has undergone extraordinary digital transformation over the past two decades, evolving from paper-based records and manual clinical processes to one of the most technologically advanced, data-driven sectors globally. The global digital health market reached an estimated value of $657.7 billion by 2026, up from approximately $175.6 billion in 2021. Simultaneously, investments in AI-driven drug development exceeded $13.8 billion in 2021, marking a dramatic increase from previous years [1]. According to a 2024 study by Microsoft and IDC, approximately 79% of healthcare organisations actively use AI systems, achieving an average return of $3.20 per dollar invested in AI technologies [2]. One of the most significant developments has been the growth of electronic clinical trial systems and Electronic Medical Records (EMRs). EMRs now manage patient recruitment, adverse reaction monitoring, regulatory submissions, and trial outcome analysis, enhanced by AI, machine learning, and natural language processing [3]. Decentralised clinical trials based on digital platforms and remote patient monitoring applications have improved accessibility but introduced significant cybersecurity risks [4]. Pharmaceutical companies have become attractive targets for cybercriminals due to the high value of healthcare data, clinical trial information, and intellectual property. According to IBM's 2023 Data Breach Report, the pharmaceutical industry experienced the highest data breach costs at an average of $4.82 million per incident. In February 2024, Cencora, a major American pharmaceutical distributor, suffered a ransomware attack that breached private health information of more than 1.43 million people, affecting at least 27 pharmaceutical firms including Bayer, Novartis, and GlaxoSmithKline [5]. The COVID-19 pandemic intensified pharmaceutical cybercrime as vaccine development became a cyber espionage target. State-sponsored hacking groups targeted pharmaceutical firms, research labs, and health agencies from multiple countries. Confidential regulatory documents concerning the Pfizer/BioNTech COVID-19 vaccine were stolen from the European Medicines Agency (EMA) and leaked online, demonstrating the link between healthcare cybersecurity and national security [6].

Data tampering represents one of the most serious cybercrime types in healthcare, including falsification of clinical data, inadequate documentation, and unauthorised changes to electronic data. Such manipulation can cause unsafe drugs to enter the market, compromise patient safety, and erode public trust. Despite these threats, the pharmaceutical industry lacks adequate forensic readiness, technical infrastructure, and cybersecurity governance [7].

This research examines how digital forensics and AI-related technologies can address pharmaceutical cybercrime, focusing on four key questions: What is the impact of cybercrime on pharmaceutical data integrity? How can AI assist cyber forensic investigations? Can blockchain enhance pharmaceutical authentication? What legal issues surround digital evidence in healthcare systems?

2. Understanding Pharmaceutical Cybercrime

2.1 Definition and Nature

Pharmaceutical cybercrime encompasses criminal activities using digital technologies, computer networks, and the internet directed at the pharmaceutical and healthcare sectors. These crimes include theft of confidential research data, falsification of clinical trial results, online sales of counterfeit drugs, ransomware attacks on hospital systems, and corporate espionage for drug formulas and vaccine research. Unlike traditional cybercrimes, pharmaceutical cybercrime directly affects human health and life beyond purely monetary consequences [8].

2.2 Types of Pharmaceutical Cybercrime

a. Clinical Trial Data Manipulation: Clinical trials determine drug safety and efficacy before public release. Data alteration can devastate patient health. In April 2016, the US FDA warned Semler Research, an Indian contract research organisation, about data integrity issues in bioequivalence studies crucial for regulatory clearance. Manipulated data distorts the scientific foundation upon which drug efficacy and safety are evaluated, eroding public trust [9].

b. Counterfeit Drug Networks: The estimated global market for counterfeit pharmaceuticals is $200 billion annually, with prevalence reaching 30-60% in developing countries. Operation Pangea IV (2011) seized 2.4 million counterfeit pills from 43 countries, shut down 13,500 websites, and inspected 45,000 packages. A $250 million US pharmaceutical scandal involved counterfeit HIV drugs with fake labels and documentation entering legitimate supply chains [10].

c. Theft of Intellectual Property: Pharmaceutical IP including drug formulas, manufacturing processes, and vaccine research represents years of scientific research and billions in investment. During COVID-19, the FBI revealed Chinese military-backed hackers probed US vaccine development organisations. The NotPetya cyberattack caused an estimated $1.3 billion damage to Merck & Co. in 2017 [11].

d. Ransomware Attacks on Healthcare Infrastructure: Ransomware encrypts victim data and demands payment for decryption. In 2025, the FBI's IC3 reported 278 ransomware attacks against the healthcare sector, the highest of all critical infrastructure sectors. Attacks increased by 30% in 2024, with 130 attacks against pharmaceutical manufacturers during the first nine months of 2025. The May 2021 Irish Health Service Executive attack caused radiotherapy service suspensions in five major centres [12].

2.3 Impact on Public Health and Consumer Safety

Manipulated clinical data can lead to approval of unsafe medications. WHO estimates approximately 10% of medical products in low- and middle-income countries are substandard or falsified, including anti-malarial drugs and antibiotics. Counterfeit drugs can cause harmful side effects, treatment failure, and death. The Change Healthcare breach cost UnitedHealth Group between $2.3 and $2.45 billion in 2024, encompassing data breach response, operational disruption, regulatory penalties, and reputational damage [13].

3. Digital Forensics in Pharmaceutical Investigations

3.1 Concept of Digital Forensics

Digital forensic science focuses on recovering and investigating digital evidence from devices related to cybercrime. The National Institutes of Health reports digital evidence appears in nearly 90% of criminal cases, demonstrating the growing importance of digital forensics in modern investigations [14]. The pharmaceutical industry relies on digital forensics to discover fraud, clinical trial data tampering, counterfeit drug networks, and cyber theft of intellectual property.

3.2 Types of Digital Evidence in Pharmaceutical Systems

Digital evidence in pharmaceutical systems includes Electronic Health Records (EHRs), which may show tampering or unauthorised access; clinical trial databases documenting drug testing and outcomes; emails and cloud storage containing sensitive research documents; and medical devices connected through the Internet of Things (IoT), including smart infusion pumps and patient monitoring devices that create data logs reconstructing events in medication errors or deliberate harm [15].

3.3 Stages of Digital Forensic Investigation

The investigation process comprises five structured stages. Identification locates potential digital evidence sources including servers, computers, medical devices, and cloud accounts. Preservation safeguards identified evidence through chain of custody protocols to prevent alteration or destruction. Collection involves carefully gathering evidence from sources using

forensic copies. Examination and Analysis interpret the collected data to determine what occurred, who was responsible, and how the crime was committed. Reporting presents findings to regulatory agencies, courts, or law enforcement in accessible language [16].

3.4 Challenges in Pharmaceutical Digital Forensics

Key challenges include encryption making data difficult to access; cross-border data storage creating jurisdictional complexities where data resides in different legal systems; chain of custody issues that may exclude evidence from trial if mishandled; and privacy concerns requiring a balance between investigation needs and patient rights under GDPR or HIPAA [17].

3.5 Role of Forensic Laboratories and Experts

AI and machine learning are emerging as transformative technologies enhancing digital forensics effectiveness through data collection, cybercrime timeline reconstruction, big data analysis, pattern recognition, chain-of-custody protection, and response strategy orchestration. The US FDA's Office of Criminal Investigations created the Pharmaceutical Fraud Program and Digital Forensics Unit specifically for pharmaceutical, biologic, and medical device investigations, handling crimes from counterfeit drugs to clinical trial fraud [18].

4. Artificial Intelligence in Pharmaceutical Fraud Detection

AI has become the primary means of detecting and preventing pharmaceutical fraud. Machine learning algorithms process vast healthcare data in real time to detect unauthorised access, billing irregularities, and unusual drug-related transactions without suffering human fatigue [19]. Cyberattacks on healthcare systems increased from 304 in 2022 to 624 in 2023, demonstrating the necessity of AI-powered predictive security systems [20]. Anomaly detection systems identify unusual patterns in clinical records, pharmaceutical transactions, and drug distribution data, flagging suspicious activities including abnormal prescription volumes, duplicate patient records, unusual billing codes, and mismatched drug-disease relationships. Research indicates nearly 10% of healthcare expenditure is lost due to medical fraud and abuse. Studies confirm AI-based systems, including clustering techniques and autoencoders, are highly effective in pharmaceutical manufacturing and distribution [21].

AI protects clinical trial integrity by detecting fabricated or manipulated data through statistical anomalies difficult for humans to recognise manually. A study in Therapeutic Innovation & Regulatory Science (2021) demonstrated AI-based statistical monitoring software successfully identified a fraudulent clinical trial centre after analysing only a small portion of submitted data. Tools such as Medidata Detect analyse irregular patterns including duplicate patient enrolments, unusual patient visit timings, and repeated numerical values indicating falsified records [22].

Deep learning models, including Convolutional Neural Networks (CNNs) combat counterfeit medicines by analysing pharmaceutical packaging for minor differences in labels, barcodes, seals, fonts, and colour patterns invisible to the human eye. IEEE (2024) research demonstrated that AI-based image recognition successfully distinguishes authentic medicines from counterfeit products, with BMC Health Services Research reporting accuracy levels above 90% [23]. However, AI systems face limitations including algorithmic bias, where AI reproduces historical inaccuracies (a Science 2019 study found a healthcare algorithm assigned equal risk scores to Black and White patients despite Black patients being significantly sicker); false positives, incorrectly flagging legitimate records; data dependency on training data quality; and "black box" opacity, making decisions difficult to understand [24].

AI use raises ethical concerns regarding privacy, data security, and automated decision-making accountability. Legal frameworks such as GDPR and HIPAA provide some protection, but accountability for AI errors remains unresolved. AI should complement rather than replace human judgment in pharmaceutical cybersecurity [25].

5. Blockchain Technology and Pharmaceutical Authentication

Blockchain technology, initially developed for cryptocurrency transactions, has become an important tool for addressing pharmaceutical fraud, counterfeit medicines, and data manipulation. Unlike centralised databases, blockchain works through a decentralised digital ledger where records are distributed across multiple network nodes. Each transaction is secured using cryptographic hash values, making unauthorised changes immediately visible, improving transparency, security, and trust [26]. In blockchain-enabled systems, every medicine batch receives a unique digital identity recording manufacturing date, expiry date, ingredients, and production source. Every supply chain movement is permanently recorded, making counterfeit medicines easier to identify. A systematic review in PeerJ Computer Science (2022) found blockchain's decentralisation, transparency, and immutability make it highly effective in reducing counterfeit drug circulation. The PharmaChain framework published in Heliyon (2023) demonstrated blockchain and smart contracts can securely manage pharmaceutical transactions and verify drug provenance [27].

Smart contracts are self-executing digital agreements stored on blockchain systems that automatically perform actions when specific conditions are satisfied. In pharmaceutical supply chains, these contracts verify quality checks,

monitor temperature-sensitive drugs during transportation, and prevent expired products from moving further in distribution. Research in Multimedia Tools and Applications (2023) described Ethereum-based blockchain systems using smart contracts to automate compliance and securely store pharmaceutical records [28].

Research in Pharmaceutical Research (2026) reported blockchain could potentially reduce counterfeit medicine circulation by nearly 40%, significantly improving patient safety and pharmaceutical governance. Blockchain strengthens evidence integrity in clinical trials by creating immutable, time-stamped records. Major pharmaceutical companies including Pfizer, Novartis, Merck, and Boehringer Ingelheim have adopted blockchain systems for clinical trial management and anti-counterfeiting measures [29].

Challenges include **cost** requiring significant investment in infrastructure and training; regulatory uncertainty regarding data ownership, liability, and GDPR compliance; and technical limitations affecting scalability, interoperability, and integration with existing healthcare systems [30].

6. Legal and Regulatory Framework

6.1 Digital Evidence and Pharmaceutical Litigation

Digital evidence is central to pharmaceutical litigation involving fraud, data manipulation, and product liability. For digital evidence to be admissible, it must satisfy four conditions: authenticated origin linking the record to a verified source and timestamp; proven integrity confirming no alteration after capture; documented chain of custody recording every access event; and compliance with applicable legal frameworks. Blockchain records and AI-generated fraud detection outputs are subject to the same admissibility standards as traditional physical evidence [17].

6.2 International Legal Frameworks

GDPR (European Union): Classifies health data as a special category requiring heightened protection and explicit patient consent, with fines up to €20 million or 4% of global annual turnover. GDPR provides individuals the right not to be subject to decisions based solely on automated processing, with significant implications for AI-driven fraud detection [32].

HIPAA (United States): Requires administrative, physical, and technical safeguards for electronic Protected Health Information (PHI), regular risk assessments, and breach notification. The 2023 HIPAA Security Rule establishes national safeguards for confidentiality, integrity, and availability. Some pharmaceutical data falls within HIPAA while some falls outside, creating regulatory complexity [7].

WHO Digital Health Guidelines: Provides normative international framework for responsible digital health implementation, influencing regulatory policy globally despite not being legally binding [5].

6.3 Indian Legal Framework

Information Technology Act, 2000: Sections 65 and 66 address computer-related offences including tampering with computer source documents, directly relevant to pharmaceutical data fraud. The IT Act provides legal basis for electronic record admissibility in Indian courts [8].

Digital Personal Data Protection Act, 2023: India's first comprehensive cross-sectoral data protection law, introducing informed consent requirements, purpose-based limitations, data minimisation, and a Data Protection Board of India with investigative and penalty powers [10].

Drugs and Cosmetics Act, 1940: Primary statute governing drug manufacture, sale, distribution, and import in India, enforced by the Central Drugs Standard Control Organisation (CDSCO), with criminal penalties for fraudulent misrepresentation of drug quality or identity [16].

Bharatiya Sakshaya Adhiniyam, 2023 (effective July 2024): Fundamentally modernised electronic evidence treatment in Indian courts. Section 61 states electronic records shall have the same legal effect as other documents. Section 63 requires certification by a responsible official and an expert, adding formal expert certification layers strengthening authenticity and accountability in pharmaceutical fraud cases [25].

6.4 Cybersecurity Governance in Pharmaceutical Industries

Pharmaceutical companies face extensive cybersecurity governance obligations including technical safeguards, risk assessments, staff training, access controls, encryption, and incident response procedures. The EU's Network and Information Security Directive (NIS2) and Cyber Resilience Act (CRA, applicable 2027) impose mandatory controls. The US SEC now requires public companies to disclose material cybersecurity incidents within four business days [16].

The EU's new Product Liability Directive (Directive 2024/2853), effective December 2026, expands "product" definition to explicitly include software and AI systems, making pharmaceutical manufacturers strictly liable when defective AI-driven systems cause harm. The Directive introduces presumption of causation for technically complex products including AI systems. The EU AI Act (effective August 2024) classifies healthcare AI systems as high-risk, requiring enhanced transparency, human oversight, and documentation. However, accountability gaps remain for black-box models, proof of causation, and continuously learning AI systems [25].

7. Case Studies

a. COVID-19 Vaccine Data Cyberattack (December 2020): Hackers accessed confidential EMA regulatory documents from Pfizer, BioNTech, and Moderna relating to COVID-19 vaccine approvals, leaking materials on online hacking forums. The forensic investigation confirmed limited document access and no personal data exposure, but raised serious GDPR concerns and highlighted cybersecurity responsibilities of healthcare regulators. The case demonstrated that vaccine research data is a valuable target for cybercriminals and geopolitical actors [6].

b. WannaCry Attack (May 2017): The ransomware spread across more than 150 countries, severely affecting the UK's National Health Service (NHS). Hospitals experienced cancelled appointments, delayed emergency services, and critical system shutdowns. Digital forensic investigations revealed spread through vulnerable Server Message Block (SMB) ports rather than email phishing, and affected systems had failed to install security updates released by Microsoft two months earlier. The attack exposed serious weaknesses in healthcare cybersecurity governance [12].

c. Counterfeit Drug Supply Chains: Research found counterfeit drugs may account for nearly 50% of medicines sold through unregulated online platforms, with approximately 95% of websites selling prescription medicines operating illegally. Companies including Gilead Sciences and Johnson & Johnson filed lawsuits against distributors involved in HIV medication tampering and repackaging schemes. Digital forensic investigations involved tracing drug distribution records, analysing lot numbers, and monitoring dark web marketplaces [10].

d. e-Research Technology (ERT) Ransomware Attack (September 2020): The software company providing digital systems for hundreds of clinical trials suffered a major ransomware attack affecting clinical trial operations for IQVIA and Bristol Myers Squibb, including COVID-19 vaccine studies. The attack locked researchers out of systems, forcing return to manual paper-based recordkeeping. ERT shut down affected systems and engaged cybersecurity experts. The incident highlighted vulnerability of third-party clinical trial vendors and reinforced the importance of forensic readiness, secure backups, and strict vendor cybersecurity assessments [5].

8. Recommendations and Policy Suggestions

The following recommendations emerge from this research. **First**, strengthen pharmaceutical cybersecurity through mandatory cybersecurity audits for pharmaceutical companies, clinical trial organisations, and supply chain participants, with strict penalties for non-compliance. **Second**, adopt AI-based monitoring systems across digital infrastructure with independent testing for transparency, reliability, and fairness. AI systems should have effective human oversight [19].

Third, establish digital forensic readiness within pharmaceutical institutions through dedicated forensic response teams, evidence preservation systems, and standardised procedures following ISO/IEC 27043. **Fourth**, introduce legal reforms with clear AI accountability laws defining responsibility for AI errors or detection failures, and strengthen international cooperation under frameworks such as the Budapest Convention on Cybercrime [25].

Fifth, encourage blockchain technology adoption for pharmaceutical supply chain transparency and drug traceability, providing technical support for smaller organisations. **Sixth**, build capacity through specialised training programmes in digital forensics, AI auditing, and healthcare cybersecurity for judicial officers, prosecutors, and regulators [29].

9. Conclusion

Pharmaceutical cybercrime has emerged as a serious threat to public health, healthcare governance, and pharmaceutical security worldwide. Cyberattacks against the EMA during the COVID-19 vaccine rollout, the WannaCry NHS attack, counterfeit drug networks, and clinical trial software attacks demonstrate that even technologically advanced organisations remain vulnerable. These incidents have serious consequences for healthcare institutions, patients, and public trust.

AI-driven solutions are increasingly valuable for recognising suspicious activity, validating clinical trial information, and combating counterfeit drugs. However, algorithmic bias, lack of transparency, prediction inaccuracy, and data quality dependence remain significant concerns. AI should complement rather than replace human judgment in pharmaceutical cybersecurity investigations.

Current laws remain fragmented and inadequate to address pharmaceutical cybercrime's magnitude. No comprehensive international legal instrument exists for pharmaceutical cybersecurity regulation. Investigations and enforcement frequently span national boundaries, requiring international collaboration that current legal frameworks inadequately support.

A multi-faceted collaborative strategy combining robust laws, sophisticated technologies (AI monitoring, blockchain verification), trained forensic experts, and strong governance is essential for ensuring long-term pharmaceutical security in the digital era. Technology alone cannot eradicate pharmaceutical cybercrime, nor can legal regulation alone fix the problem. Only an integrated approach will secure healthcare systems for the future.

10. References

1. Markets and Markets. Digital health's future in pharma and healthcare trends. 2025.

2. BenchSci. AI in drug development surpassed $13.8 billion in 2021. 2022.
3. Advancements in electronic medical records for clinical trials: enhancing data management and research efficiency. *PubMed Central*. 2025.
4. Reenalda J, et al. The digital platform and its emerging role in decentralized clinical trials. *J Med Internet Res*. 2024;26:e47882.
5. Censinet Inc. Pharmaceutical forensics: data breach analysis. 2025.
6. Pharmaceutical Technology. Pharma cyber attacks: five breaches that the industry must learn from. 2022.
7. Chernyshev M, Zeadally S, et al. Healthcare data breaches: implications for digital forensic readiness. *J Med Syst*. 2019.
8. Pharmaceutical Technology. Cybercrime in the pharmaceutical industry: a booming business. 2012.
9. Ensuring data integrity in the pharmaceutical lifecycle: challenges, principles, and global implications. *Int J Pharm*. 2025.
10. Bhole R, More RP, Nikam Y, More V, Bhatkhande R, Raskar I. The role of digital forensics in cybercrime investigations: methods, tools, and legal considerations. In: Tuba M, Akashe S, Joshi A, editors. *ICT systems and sustainability*. Cham: Springer; 2026. (Lecture Notes in Networks and Systems; vol 1645).
11. Help Net Security. Attackers are coming for drug formulas and patient data. 2025.
12. Jardine E, et al. Cyberbiosecurity in the new normal: cyberbio risks, pre-emptive security, and the global governance of bioinformation. *Eur J Int Secur*. 2024.
13. Borghesi A, et al. AI-induced cybersecurity risks in healthcare: a narrative review of blockchain-based solutions within a clinical risk management framework. *PMC*. 2025.
14. Alenezi AM. Digital forensics in the age of smart environments: a survey of recent advancements and challenges. *arXiv*. 2023.
15. Servida F, Casey E. IoT forensic challenges and opportunities for digital traces. *Digit Investig*. 2019;28:S22-S29.
16. Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. *Int J Comput Sci Secur*. 2011;5(1):118-31.
17. Casino F, Dasaklis TK, Spathoulas GP, et al. Research trends, challenges, and emerging topics in digital forensics: a review of reviews. *IEEE Access*. 2022;10.
18. U.S. Food and Drug Administration. OCI history – Office of Criminal Investigations [Internet]. [cited 2026 Jun 2]. Available from: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/who-we-are/oci-history
19. Al-Ghamdi A, et al. Artificial intelligence: cybersecurity threats in pharmaceutical. In: *2024 ASU International Conference on Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*. 2024.
20. International Social Security Association. Detecting fraud in health care through emerging technologies. 2022.
21. Zhang C, Xiao X, Wu C. Medical fraud and abuse detection system based on machine learning. *Int J Environ Res Public Health*. 2020;17(19):7265.
22. Clinical Leader. Global AI in clinical trials: market trends & current partnerships. 2025.
23. Grand View Research. AI in healthcare market size & share | industry report, 2033. 2024.
24. Losavio M, Chow KP, Koltay A, James J. The Internet of Things and the smart city: legal challenges with digital forensics, privacy, and security. *Secur Priv*. 2018;1(3):e23.
25. Casey E. *Digital evidence and computer crime: forensic science, computers and the internet*. 3rd ed. London: Academic Press; 2011.
26. Rathod S. Cloud forensics: a framework for investigating cyberattacks in cloud environments. *IJCSNS*. 2017;17(6).
27. Zimmermann C, Kohn M. The digital forensic investigation model for pharmaceutical cyber fraud. *Forensic Sci Int Digit Investig*. 2012.
28. Garfinkel SL. Digital forensics research: the next 10 years. *Digit Investig*. 2010;7(Supplement):S64-S73.
29. ResearchGate. The evolution of cybersecurity law: global approaches to combating cybercrime. 2025.
30. Future Market Insights. Digital transformation in healthcare market size, share & analysis 2025–2035 [Internet]. [cited 2026 Jun 2]. Available from: https://www.futuremarketinsights.com/reports/digital-healthcare-market