"Data Privacy and Security in the Age of Digital Transformation in Pharma"

Ravindra Prasad Gupta[1], Pratiksha Tembhurkar[2], B. Lakshmi[3], SaiKishore V[4]

[1]MBA, Pharmaceutical Management, NIPER Hyderabad India

[2]MBA, Pharmaceutical Management, NIPER Hyderabad India

[3]Assistant Professor, NIPER, Hyderabad India

[4]Assistant Professor, NIPER, Hyderabad India

Abstract

In the age of digital revolution, the pharmaceutical sector is transforming dramatically, adopting cutting-edge technologies to enhance patient care, clinical trials, and drug discovery. But this change is not without its difficulties, especially when it comes to data security and privacy. The risk of data breaches and unauthorised access has never been higher, as the sector depends more and more on large volumes of sensitive patient data, intellectual property, and research discoveries. This review article explores the implications of strict data protection regulations, the evolving threat landscape, and effective methods for protecting sensitive information. It also delves into the critical aspects of data privacy and security in the age of digital transformation in the pharmaceutical industry.

Keyword : *Cybersecurity, Privacy Policies, Data Breach, Cyber Threats, Data Governance, Digital transformation, Threat Intelligence, Blockchain, Secure Communication.*

Introduction

In the wake of the digital revolution sweeping through the pharmaceutical industry, characterized by the integration of advanced technologies and expansive datasets, the sector finds itself at the forefront of transformative innovation Digital transformation in pharma, encompassing artificial intelligence (AI), big data analytics, and interconnected platforms, promises accelerated drug development, personalized healthcare solutions, and improved patient outcomes (Hie et al., n.d.).

Amidst the promise of these technological advancements, a critical concern looms large—the need to secure sensitive healthcare data in an era marked by escalating cyber threats and unauthorized access Patient records, clinical trial information, and proprietary research data constitute a treasure trove of valuable and sensitive information that necessitates robust protection across the pharmaceutical value chain (MacKey & Nayyar, 2016).

The unique nature of pharmaceutical data, coupled with the intricate web of stakeholders involved in drug development and distribution, amplifies the complexity of data privacy and security challenges. As the industry pivots towards a future driven by data, it confronts the imperative to strike a delicate balance between leveraging the transformative potential of digital innovation and fortifying defenses against potential breaches and cyber-attacks (Yaqoob et al., 2022a).

This review endeavors to navigate this dynamic landscape, shedding light on the multifaceted dimensions of data privacy and security in the age of digital transformation in the pharmaceutical industry. By examining current challenges, regulatory frameworks, industry standards, and emerging best practices, the review aims to provide a comprehensive guide for industry stakeholders, regulatory bodies, and technology experts in navigating the evolving terrain of pharmaceutical innovation securely**.**(Huang et al., n.d.-a)

Review of literature

Current state of data privacy practices in Pharmaceutical industry

Patients' private information is frequently compromised by data breaches, even in spite of the increased attention being paid to the security of electronic health records and the efforts of large cities worldwide to implement smart city infrastructure. Current record management systems have difficulty striking a balance between patient and provider regular data interaction requirements and data privacy**.** (Luthans, 2011).

Drug traceability systems, which track or trace where a drug has been and where it has gone along the drug supply chain, are fundamental to pharmaceutical companies' business and public drug security. The shortcomings of traditional centralized server-client technical solutions in terms of data authenticity, privacy, system resilience, and adaptability have made them far from satisfactory. Centralized systems are susceptible to unapproved access and data manipulation, which jeopardizes the veracity of information about drug transactions. A single breach can reveal a significant amount of private data, which is why storing sensitive information in a centralised database raises privacy issues. A great degree of adaptability is required because to the rapid changes in rules, technology, and business requirements; centralized systems find it difficult to achieve this. (Huang et al., n.d.-a).

Blockchain technology offers a decentralized, impenetrable platform for recording and validating transactions, which has the potential to improve data privacy and security in pharmaceutical supply chain management (SCM). It provides tamper-proof security, scalability, and eliminates the need for a third party to be trusted. Additionally, this technology can lower healthcare expenses, protect patient privacy in medical records, and enhance audibility through the development of immutable logs**.** (De Aguiar et al., 2020) **.**

Large private datasets of DTIs, along with corresponding chemical structures and protein sequences, are held by (e.g., pharmaceutical companies or research laboratories). These entities first pool their data using secret sharing, which conceals information about the underlying drugs, targets, or interactions (step 1). After that, the cooperating parties carry out a cryptographic procedure together that uses the pooled dataset to build a predictive model (like a neural network) (step 2) The finished model can be distributed to participants in a form that promotes increased data exchange, or it can be made available to participating companies (step 3) (Hie et al., n.d.).

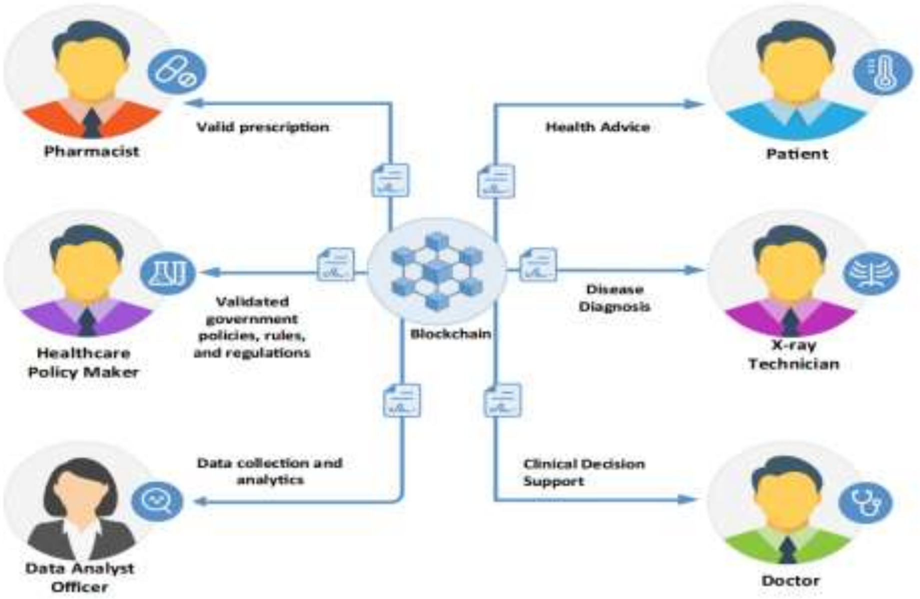


Fig. 1. Secure pipeline for pharmacological collaboration. Collaborating entities (Yaqoob et al., 2022a).

Main risks and weaknesses in data privacy that pharmaceutical companies need to address

While patient safety problems related to illegal internet pharmacies are undoubtedly the most urgent social issues, cybersecurity and privacy concerns should also be taken into consideration when evaluating consumer protection measures. A 2011 study that examined 60 online pharmacy websites revealed that the majority (80%) had either critical or medium-level vulnerabilities that do not offer sufficient safety for online customers. This suggests that there may be a hazard to online consumers. 65 In a similar vein, the National Association of Boards of Pharmacy (NABP) discovered that 17% of the online pharmacies they looked at didn't have a secure website**.** (MacKey & Nayyar, 2016).

The hazards of cybersecurity and the accessibility of malicious applications in the data of IoT systems have generally increased due to a variety of actions, including forgetting to change passwords, being unaware of our surroundings, and not updating our devices. The probability of a data breach and other security vulnerabilities is increased by these attacks and intrusions into the IoT data system**.** (Chong et al., n.d.).

The Ali mobile security team discovered that over 90% of IoT device firmware had security flaws including hard-coded keys and basic Web security flaws, which might be readily exploited by attackers. This is because many new IoT device types lack adequate safety tests beforehand**.** (Zhou et al., 2019).

Technical or technological threats: Research has even suggested that security and authorization in blockchain technology are interconnected problems. According to three studies, blockchain technology is vulnerable to cyberattacks like mempool attacks, which occur when a large number of transactions flood a block and take over most blockchain networks, and domain name system (DNS) attacks. (Abu-elezz et al., 2020).

Social threats: According to three studies, the main hindrance to the extensive implementation of blockchain technology was the public's acceptance of it. The decentralization of medical data and the disengagement of a reliable third party make it challenging for the government to grant access, underscoring privacy as a valid concern**.** (Abu-elezz et al., 2020).

Organizational threats: Research revealed that one of the main challenges in implementing blockchain technology in the healthcare industry is interoperability. Studies have linked interoperability issues to low open standards and a lack of trust between parties, which make it difficult for healthcare organizations to fully communicate patient data**.** (Abu-elezz et al., 2020).

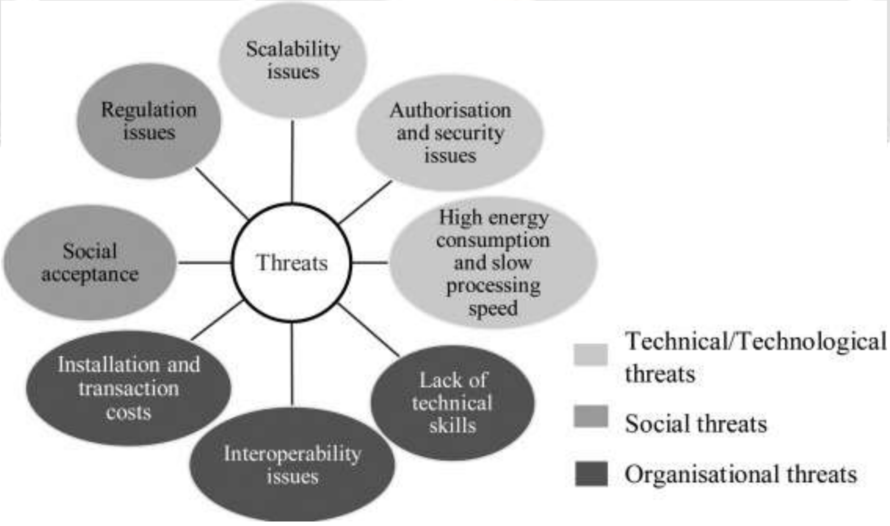

Scalability issues
Regulation issues
Authorisation and security issues
Social acceptance
Threats
High energy consumption and slow processing speed
Installation and transaction costs
Lack of technical skills
Interoperability issues
Technical/Technological threats
Social threats
Organisational threats

Fig. 2. Three groups of eight blockchain dangers were identified: social threats (social acceptance and regulatory issues), organisational threats (installation and transaction costs, lack of technical skills, and interoperability issues), and technological threats (scalability issues, authorisation and security issues, high energy consumption, and slow processing speeds).(Abu-elezz et al., 2020).

Effects of data breaches on a pharmaceutical company's credibility and reputation

It's challenging to stop breaches of medical data. Networked healthcare systems require the sharing of data between many platforms and devices, AI "fits into already-existing legal categories, or if a new category with its own unique characteristics and repercussions needs to be created?"is a topic of ongoing discussion. While there is much hope that using AI in clinical settings would enhance healthcare, there are also moral concerns that need to be addressed. (Barenji et al., 2019).

AI in healthcare has four main ethical concerns that need to be resolved in order to reach its full potential: Concerns of (1) informed consent to utilize data(2) security and openness; (3) algorithmic biases and fairness; and (4) privacy of dataare all crucial. ch raises the risk of exposure and security breaches for the company. Intrusive cyber agents can corrupt, steal, or modify patient data, which can harm patients when the data is used for medical treatment or when the stolen data is used for identity theft.(McLeod & Dolezel, 2018).

One of the biggest security breaches that have happened recently was The US retailer Target in 2014, which involved an estimated 70 million credit card records; JP Morgan Chase in 2014, which involved 76 million accounts; and Anthem in early this year, which resulted in the loss of client and employee personal information, are among the most recent significant security breaches. Another example would be an infusion pump that gives a patient a predetermined amount of fluids into their body. The dosage that is administered could be altered by an unauthorized person using this device. (Pharma et al., 2017)**.**

AI "fits within existing legal categories or whether a new category with its special features and implications should be developed?" is a topic of ongoing discussion. While there is much hope that using AI in clinical settings would enhance healthcare, there are also moral concerns that need to be addressed. AI in healthcare has four main ethical concerns that need to be resolved in order to reach its full potential: Concerns of (1) informed consent to utilize data, (2) safety and transparency, (3) algorithmic fairness and biases, and (4) data privacy are all crucial**.** (Naik et al., 2022).

Stakeholder perceptions of data privacy in the pharmaceutical industry

- **Patients:** Patients are increasingly concerned about the privacy of their health data. (Wetzels et al., 2018)A 2022 survey by Deloitte found that 83% of patients are concerned about how their health data is used by pharmaceutical companies. Patients are particularly concerned about the use of their data for marketing purposes and the sharing of their data with third-party vendors.(Shen et al., 2019).

- **Healthcare providers:** Healthcare providers are also concerned about the privacy of their patients' health data. A 2023 survey by the American Medical Association found that 90% of physicians are concerned about the privacy of their patients' data when sharing it with pharmaceutical companies. Healthcare providers are particularly concerned about the use of their patients' data for clinical trials and the sharing of their data with third-party vendors.(Adarmouch et al., 2020).

- **Regulators:** Regulators are also concerned about the privacy of patient health data. The US Food and Drug Administration (FDA) has issued guidance on the collection and use of patient data by pharmaceutical companies. The FDA guidance requires pharmaceutical companies to obtain informed consent from patients before collecting their data and to use the data only for the purposes for which it was collected.(Huang et al., n.d.-b).

Regulatory landscape governing data privacy in the pharmaceutical sector

The pharmaceutical sector is one of the most highly regulated industries in the world, and data privacy is a key area of focus for regulators. This is because pharma companies collect and store a vast amount of sensitive data, including patient health information, intellectual property (IP), and financial data.(Miller et al., 2021) This data is a valuable target for cybercriminals, who are increasingly sophisticated and well-resourced.

Key data privacy regulations in the pharmaceutical sector:

The following are some of the key data privacy regulations that apply to the pharmaceutical sector:

1. **General Data Protection Regulation (GDPR):** A rule under EU law pertaining to data protection and privacy that applies to all citizens of the EU and the EEA is known as the General Data Protection Regulation (GDPR) (EEA). It also covers the transmission of personal information outside of the EEA and EU. Individuals have the right under the GDPR to access, correct, erase, and limit the processing of their personal data. Additionally, before collecting or processing an individual's personal data, organisations must get that individual's consent (Tucker et al., 2016).

2. **California Consumer Privacy Act (CCPA):** The California Civil Process Act (CCPA) governs how personal information on citizens of California is gathered, used, and disclosed. Under the CCPA, people have the right to know what personal information companies gather about them, the right to ask for that information to be deleted, and the right to refuse to have their personal information sold (Mulgund et al., 2021).

3. **Health Insurance Portability and Accountability Act (HIPAA):** The privacy of personally identifiable health information is safeguarded under US law known as HIPAA. HIPAA mandates the use of security measures to preserve the privacy, accuracy, and accessibility of protected health information by covered organisations, including medical facilities and insurance providers (Lyapustina et al., 2018).

4. **Clinical Trials Regulation (EU No 536/2014):** The Clinical Trials Regulation (CTR) is a regulation in EU law on the conduct of clinical trials for medicinal products for human use. It includes provisions on the protection of personal data collected in clinical trials. The CTR requires sponsors of clinical trials to implement measures to protect the confidentiality and security of personal data collected in clinical trials (Fortunato et al., 2018).

5. **The Personal Data Protection Bill, 2019:** The impending enactment of the Personal Data Protection Bill, 2019 in India is set to have a substantial impact on data privacy within the pharmaceutical sector. This legislation introduces stringent data protection principles, emphasizing consent-based processing and safeguards for sensitive healthcare data. It also requires data localization, cross-border data transfer compliance, and robust data breach reporting mechanisms.(Singh & Ruj, 2020).

   Pharmaceutical companies must adapt to these regulations, appoint Data Protection Officers, conduct Data Protection Impact Assessments, and establish transparent consent mechanisms to ensure compliance, protect patient privacy, and mitigate potential penalties for non-compliance.(Martin et al., 2019).

Innovative technologies and strategies for enhancing data privacy

As the amount of data collected and stored increases, so does the risk of data breaches and other privacy violations. Innovative technologies and strategies can help to enhance data privacy by making it more difficult for unauthorized individuals to access and use personal data.(Levchenko et al., 2011).

Privacy-enhancing technologies

Privacy-enhancing technologies (PETs) are a set of tools and techniques that can be used to protect the privacy of data.(Al-Issa et al., 2019) PETs can be used to encrypt data, anonymize data, and control access to data.

Some examples of PETs include:

1. **Encryption:** Encryption scrambles data so that it can only be read by someone who has the encryption key. This can be used to protect data at rest (stored on a device) and in transit (being transmitted over a network).(Stamatellis et al., 2020).
2. **Homomorphic Encryption:** Health information that is personally identifiable is protected by US law under HIPAA. Protections against the confidentiality, integrity, and availability of protected health information must be put in place by covered entities under HIPAA, including medical facilities and health insurance providers.(Gentry, 2009).
3. **Anonymization:** Anonymization removes personal identifiers from data so that it cannot be traced back to individuals. This can be done by removing names, addresses, and other identifying information (R. Xu et al., 2021)
4. **Access control:** Access control restricts who can access and use data. This can be done by using passwords, multi-factor authentication, and other security measures (Sweeney, 2002).

Innovative strategies for enhancing data privacy

In addition to PETs, there are a number of innovative strategies that can be used to enhance data privacy. Some examples of innovative strategies for enhancing data privacy include:

1. **Data privacy by design:** Data privacy by design is a concept that emphasizes the importance of considering privacy from the outset of any data collection or processing activity. This means that privacy risks should be identified and mitigated throughout the data lifecycle (Understanding-Privacy-by-Design-A-Comprehensive-Overview, n.d.).

2. **Differential privacy:** Differential privacy has gained significant attention in recent years as a robust strategy for protecting personal data in statistical analysis and machine learning. Differential privacy adds noise to data to protect individual privacy, while still allowing for useful insights to be drawn from the aggregated data(Dwork & Roth, 2013).

3. **Federated Learning:** In the context of machine learning, federated learning is a technique that allows models to be trained across multiple decentralized devices while keeping data localized.(J. Xu et al., 2021) This approach minimizes the risk of data leakage, as the data never leaves the devices, and only model updates are shared (Konečn et al., 2016).

4. **Zero-Knowledge Proofs:** Zero-knowledge proofs have garnered interest for their ability to prove a statement without revealing any information about the statement itself. This technology is particularly relevant for authentication and access control. Recent advancements in this area, such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), have the potential to revolutionize privacy in blockchain and financial applications (Ben-Sasson et al., 2014).

5. **Blockchain Technology:** Blockchain technology is not limited to cryptocurrencies; it also has a significant role to play in data privacy (Bodkhe et al., 2020). Blockchains can offer transparent and tamper-resistant record-keeping systems, and recent research has explored their use in building privacy-preserving applications(Farouk et al., 2020). For example, Confidential Transactions and Confidential Assets are techniques within blockchain technology that enable private transactions without revealing transaction amounts or sender/receiver details (Yaqoob et al., 2022b).

6. **Multi-Party Computation (MPC):** Multi-party computation enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. Recent developments in this field have made it more practical for real-world applications, such as secure data analytics and collaborative research (Ben-David et al., 2008).

Case Study:

Cyberattacks against businesses increased dramatically during the pandemic, and the healthcare industry was no exception. Over 200 attacks explicitly related to the pandemic were recorded by the UK's National Cyber Security Centre (NCSC), which included an "almost likely" Russian intelligence service hack on vaccine research. IBM, a technology company, discovered several hacks targeting the cold chain for vaccines, notably targeting the government and commercial organizations involved in distribution. It was unclear if the offenders wanted to disrupt the deployment or steal the intellectual property. Following a cyberattack in October 2020, Indian pharmaceutical company Dr. Reddy's Laboratories was compelled to close many production facilities. In addition to closing plants in the US, UK, Brazil, India, and Russia, it isolated all data centers. The event happened right as Dr. Reddy's was preparing for the last round of trials for Russia's Sputnik V vaccine. At this stage of the epidemic, clinical trial data—an important piece of intellectual property—was present on the targeted servers. CIO "We expect all services to be up within 24 hours and we do not foresee any substantial impact on our operations owing to this occurrence," stated Mukesh Rathi**.** (Millar, 2021).

Methodology

The literature search was limited to articles published from 2008 – 2022.The search articles was done online by using the search words " Data privacy challenges ,Cybersecurity in pharma ,Regulatory compliance and data security" in the title and keywords in research databases at Wiley, Elsevier, Taylor & Francis, ERIC, Springer, SAGE, Frontiers.

Analysis

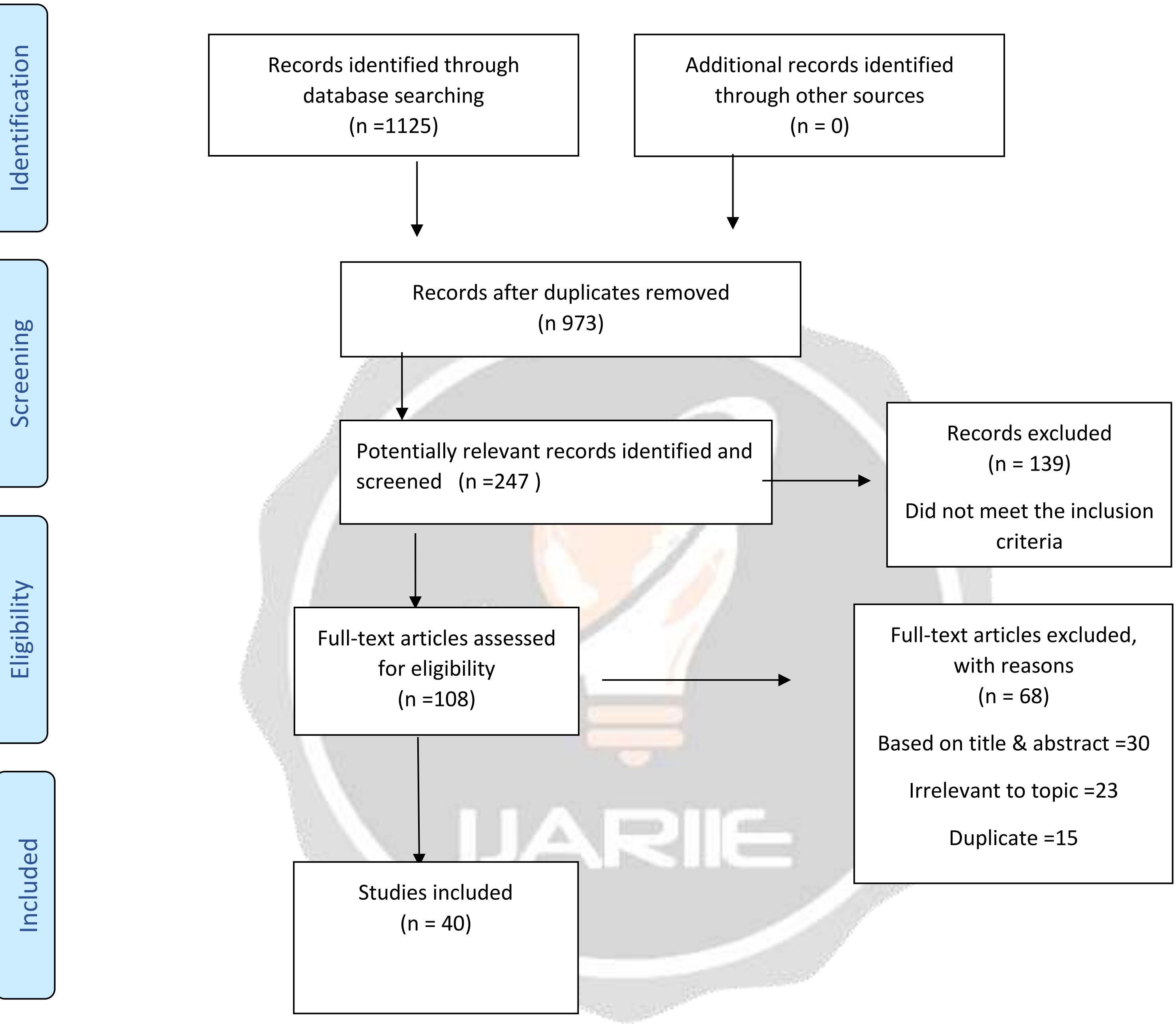
The method used is the Preferred Reporting Item for Systemic Reviews and Meta analytic (PRISMA) method. All articles that have passed the selection process were then reviewed and summarised based on the objectives, year of publication, number of citations and suggestions for further research.

Inclusion & Exclusion criteria

The be included in current study, studies have to meet some criteria

(a) Studies have included some kind of selection criteria (Data privacy, Data security and digital transformation). These criteria limited the number of studies
(b) Accordingly excluded the studies in which it based on irrelevant information there is no proper Title, Abstract & Review.

PRISMA Flow Diagram


Identification
Screening
Eligibility
Included
Records identified through database searching (n =1125)
Additional records identified through other sources (n = 0)
Records after duplicates removed (n 973)
Potentially relevant records identified and screened (n =247)
Records excluded (n = 139)
Did not meet the inclusion criteria
Full-text articles assessed for eligibility (n =108)
Full-text articles excluded, with reasons (n = 68)
Based on title & abstract =30
Irrelevant to topic =23
Duplicate =15
Studies included (n = 40)

Final data set

The research database search resulted in all keywords search results obtained 1125 research articles. After scanning the title, there was the same article in two different databases. The results after deducting the duplicates are 973 articles. A total of 247 articles were screened. 139 Articles excluded that they not meet the inclusion criteria.

Articles accessed for eligibility are 108 articles. A Total number of 48 articles excluded based on title and abstract (30) Irrelevant to topic (23) Duplicate (15).

The final data set consists of 40 articles.

The oldest included study was published in the year 2008 and the most recent study was conducted on 2022. The Entire process is shown in figure.

Discussion

The review delves into the complex terrain of data privacy practices in the pharmaceutical industry, exposing vulnerabilities despite increased attention to electronic health record security. Current record management systems struggle to balance patient-provider interactions with robust data privacy, while drug traceability systems face shortcomings in centralized solutions. Blockchain technology emerges as a promising solution, offering decentralized security. Risks in data privacy extend beyond traditional cybersecurity, encompassing illegal online pharmacies and IoT system vulnerabilities. Data breaches profoundly impact pharmaceutical companies, raising ethical concerns regarding AI applications in healthcare. Stakeholder perceptions, including patient concerns about data use, healthcare providers' worries, and regulatory guidance, shape the industry's approach. The regulatory landscape, governed by GDPR, CCPA, HIPAA, and others, demands strict compliance. Innovative technologies and strategies, from privacy-enhancing tools to blockchain applications, play a vital role. A case study highlights the tangible consequences of cyberattacks during the pandemic, underscoring the imperative for robust cybersecurity measures. In conclusion, safeguarding patient data in the pharmaceutical industry requires a multifaceted approach integrating technology, regulatory compliance, stakeholder engagement, and ethical considerations.

Conclusion

The current state of data privacy practices in the pharmaceutical industry presents challenges due to persistent data breaches and inadequate record management systems. Blockchain technology emerges as a promising solution, offering decentralized security for drug traceability. The industry faces risks such as cybersecurity threats, AI-related ethical concerns, and potential breaches with significant consequences for patient safety and clinical trials. Stakeholders, including patients, healthcare providers, and regulators, express growing concerns about data privacy.

Regulatory measures, such as GDPR, CCPA, HIPAA, and impending legislation in India, highlight the industry's commitment to compliance. To enhance data privacy, pharmaceutical companies explore innovative technologies like encryption, homomorphic encryption, and strategies such as data privacy by design and federated learning.

The case study of cyberattacks during the pandemic emphasizes the industry's vulnerability, showcasing the need for robust cybersecurity measures to protect patient data and intellectual property. The pharmaceutical industry navigates a dynamic landscape, balancing technological advancements with evolving threats. Adapting to regulations, implementing innovative solutions, and prioritizing ethical data practices are crucial for maintaining patient trust and industry credibility.

References

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. In *International Journal of Medical Informatics* (Vol. 142). Elsevier Ireland Ltd. https://doi.org/10.1016/j.ijmedinf.2020.104246

Adarmouch, L., Felaefel, M., Wachbroit, R., & Silverman, H. (2020). Perspectives regarding privacy in clinical research among research professionals from the Arab region: An exploratory qualitative study. *BMC Medical Ethics, 21*(1), 1–16. https://doi.org/10.1186/S12910-020-0456-9/TABLES/2

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). EHealth Cloud Security Challenges: A Survey. In *Journal of Healthcare Engineering* (Vol. 2019). Hindawi Limited. https://doi.org/10.1155/2019/7516035

Barenji, R. V., Akdag, Y., Yet, B., & Oner, L. (2019). Cyber-physical-based PAT (CPbPAT) framework for Pharma 4.0. *International Journal of Pharmaceutics, 567*. https://doi.org/10.1016/j.ijpharm.2019.06.036

Ben-David, A., Nisan, N., & Pinkast, B. (2008). FairplayMP - A system for secure multi-party computation. *Proceedings of the ACM Conference on Computer and Communications Security*, 257–266. https://doi.org/10.1145/1455770.1455804

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *Proceedings - IEEE Symposium on Security and Privacy*, 459–474. https://doi.org/10.1109/SP.2014.36

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A comprehensive review. *IEEE Access*, *8*, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579

Chong, C., Lee, K., & Ahmed, G. (n.d.). Improving Internet Privacy, Data Protection and Security Concerns. In *International Journal of Technology, Innovation and Management (IJTIM)* (Vol. 1, Issue 1). https://journals.gaftim.com/index.php/ijtim/issue/view/1PublishedbyGAF-TIM,gaftim.com

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A Survey of Blockchain-Based Strategies for Healthcare. In *ACM Computing Surveys* (Vol. 53, Issue 2). Association for Computing Machinery. https://doi.org/10.1145/3376915

Dwork, C., & Roth, A. (2013). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, *9*(3–4), 211–487. https://doi.org/10.1561/0400000042

Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. In *Computer Communications* (Vol. 154, pp. 223–235). Elsevier B.V. https://doi.org/10.1016/j.comcom.2020.02.058

Fortunato, A., Grainger, D. W., & Abou-El-Enein, M. (2018). Enhancing patient-level clinical data access to promote evidence-based practice and incentivize therapeutic innovation. In *Advanced Drug Delivery Reviews* (Vols. 136–137, pp. 97–104). Elsevier B.V. https://doi.org/10.1016/j.addr.2018.01.017

Gentry, C. (2009). *A FULLY HOMOMORPHIC ENCRYPTION SCHEME A DISSERTATION SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND THE COMMITTEE ON GRADUATE STUDIES OF STANFORD UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY*.

Hie, B., Cho, H., & Berger, B. (n.d.). *Realizing private and practical pharmacological collaboration*. http://science.sciencemag.org/

Huang, Y., Wu, J., & Long, C. (n.d.-a). *Drugledger: A Practical Blockchain System for Drug Traceability and Regulation*.

Huang, Y., Wu, J., & Long, C. (n.d.-b). *Drugledger: A Practical Blockchain System for Drug Traceability and Regulation*.

Konečn, J., Brendan McMahan, H., Yu, F. X., Theertha Suresh, A., Bacon Google, D., & Richtárik, P. (2016). *Federated Learning: Strategies for Improving Communication Efficiency*. https://arxiv.org/abs/1610.05492v2

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M., & Savage, S. (2011). Click trajectories: End-to-end analysis of the spam value chain. *Proceedings - IEEE Symposium on Security and Privacy*, 431–446. https://doi.org/10.1109/SP.2011.24

Luthans, Fred. (2011). *Organizational behavior : an evidence-based approach*. McGraw-Hill Irwin.

Lyapustina, S., Armstrong, K., & Drinker Biddle, J. (2018). *As appeared in Inhalation*. www.inhalationmag.com

MacKey, T. K., & Nayyar, G. (2016). Digital danger: A review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. In *British Medical Bulletin* (Vol. 118, Issue 1, pp. 110–126). Oxford University Press. https://doi.org/10.1093/bmb/ldw016

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*, *21*(6), 1307–1324. https://doi.org/10.1007/S10796-019-09974-2/FIGURES/2

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

Millar. (2021, September 17). *) Pharma cyber attacks: Five breaches that the industry must learn from, Pharmaceutical Technology*. Pharmaceutical Technology.

Miller, R., Wafula, F., Onoka, C. A., Saligram, P., Musiega, A., Ogira, D., Okpani, I., Ejughemre, U., Murthy, S., Garimella, S., Sanderson, M., Ettelt, S., Allen, P., Nambiar, D., Salam, A., Kweyu, E., Hanson, K., & Goodman, C. (2021). When technology precedes regulation: The challenges and opportunities of e-pharmacy in low-income and middle-income countries. *BMJ Global Health*, *6*(5). https://doi.org/10.1136/bmjgh-2021-005405

Mulgund, P., Mulgund, B. P., Sharman, R., & Singh, R. (2021). The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. *Health Policy and Technology*, *10*(3), 100543. https://doi.org/10.1016/J.HLPT.2021.100543

Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Brahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlosta, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers in Surgery*, *9*. https://doi.org/10.3389/fsurg.2022.862322

Pharma, J. T. J., Sci, P., & Jaithliya, T. (2017). Citation: Jaithliya T (2017) Cyber Security in Pharmacy and Pharmaceutical Companies. *J Pharma Pharma Sci*, 121. https://doi.org/10.29011/2574-7711/100021

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. In *International Journal of Medical Informatics* (Vol. 125, pp. 1–12). Elsevier Ireland Ltd. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Singh, R. G., & Ruj, S. (2020). *A Technical Look At The Indian Personal Data Protection Bill*. https://arxiv.org/abs/2005.13812v1

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors (Switzerland)*, *20*(22), 1–14. https://doi.org/10.3390/s20226587

Sweeney, L. (2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY 1. In *International Journal of Uncertainty, Puzziness and Knowledge-Based Systems* (Vol. 10, Issue 5). www.worldscientific.com

Tucker, K., Branson, J., Dilleen, M., Hollis, S., Loughlin, P., Nixon, M. J., & Williams, Z. (2016). Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Medical Research Methodology*, *16*. https://doi.org/10.1186/s12874-016-0169-4

Understanding-Privacy-by-Design-A-Comprehensive-Overview. (n.d.).

Wetzels, M., Broers, E., Peters, P., Feijs, L., Widdershoven, J., & Habibovic, M. (2018). *Patient Perspectives on Health Data Privacy and Management: (Where Is My Data and Whose Is It?)*. https://doi.org/10.1155/2018/3838747

Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated Learning for Healthcare Informatics. *Journal of Healthcare Informatics Research*, *5*(1). https://doi.org/10.1007/s41666-020-00082-4

Xu, R., Baracaldo, N., & Joshi, J. (2021). *Privacy-Preserving Machine Learning: Methods, Challenges and Directions*. http://arxiv.org/abs/2108.04417

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022a). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *34*(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022b). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *34*(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733