International Journal of Clinical and Medical Sciences (IJCMS)
Volume 1, Issue 1, Jan-Jun 2025
Page no : 20-27

Generative AI and Cybersecurity Risks in Digital Pharmacy Services

Mr. Bobin Sondhi, Mr. Surjeet Singh

Abstract

Generative Artificial Intelligence (GenAI) is emerging as an important technology in digital pharmacy services, supporting medication information, patient communication, prescription assistance, pharmaceutical research, documentation, customer support, and knowledge management. Large language models and other generative systems can process natural-language queries and produce human-like responses, creating opportunities to improve the accessibility and efficiency of pharmacy services. However, the integration of GenAI into pharmacy environments also introduces significant cybersecurity, privacy, safety, and governance risks. Unlike conventional software systems, generative AI can produce inaccurate information, disclose sensitive data, respond to malicious prompts, generate misleading content, and become vulnerable to prompt injection and data-poisoning attacks. In digital pharmacy services, these risks can become particularly serious because AI-generated information may influence medication-related decisions. This research examines the emerging cybersecurity risks associated with GenAI in digital pharmacy services and discusses governance mechanisms for responsible implementation. The study adopts a conceptual and literature-based methodology and categorizes the major risks into data privacy, prompt injection, unauthorized access, model manipulation, hallucination, misinformation, insecure integration, and supply-chain risks. The analysis suggests that GenAI should be deployed with strict access controls, privacy protection, human oversight, output validation, monitoring, and organizational governance. The study concludes that the responsible use of GenAI in pharmacy requires a balance between technological innovation, cybersecurity, patient safety, and professional accountability.

Keywords: *Generative AI, Cybersecurity, Digital Pharmacy, Large Language Models, Pharmacy Services, Data Privacy, Prompt Injection, AI Governance, Patient Safety, Artificial Intelligence.*

Received : 20.03.2025	Acceptance :26.03.2025	Publication : 28.03.2025

INTRODUCTION

Digital transformation has significantly changed the delivery of pharmacy services. Electronic prescriptions, online pharmacies, mobile health applications, electronic medication records, automated dispensing systems, cloud-based pharmacy platforms, and digital consultation services have become increasingly important components of modern pharmaceutical practice. These technologies allow pharmacists and patients to access medication-related information more efficiently and support the automation of several administrative and informational activities.

The emergence of Generative Artificial Intelligence has introduced a new stage of digital transformation. Unlike traditional analytical AI systems that primarily classify or predict outcomes, generative AI can create new content in response to natural-language instructions. Large language models can generate explanations, summaries, recommendations, reports, and conversational responses. In pharmacy environments, such capabilities can potentially support medication information services, patient education, pharmaceutical documentation, research assistance, inventory communication, and administrative activities.

For example, a digital pharmacy platform may use a generative AI assistant to answer general questions about medication schedules, explain prescription instructions in simple language, summarize pharmaceutical documents, or assist pharmacists in preparing information for patients. GenAI may also support pharmaceutical researchers by summarizing scientific literature and assisting with information discovery.

However, pharmacy is a sensitive environment because digital systems process information related to patients, medications, prescriptions, healthcare providers, and financial transactions. Therefore, the consequences of inaccurate or compromised AI outputs can be more serious than in ordinary business applications.

One major concern is the possibility of AI hallucination. A generative AI system may produce an answer that appears convincing but contains incorrect information. If a patient or pharmacy employee accepts such information without verification, it could potentially result in inappropriate medication-related decisions.

Another emerging threat is prompt injection. Attackers may construct malicious instructions that cause a generative AI system to ignore its intended rules, reveal sensitive information, or perform unintended actions. When GenAI is connected to pharmacy databases or external applications, the potential impact of such attacks becomes greater.

Data privacy is another major concern. Generative AI systems may process patient queries, prescription information, and other sensitive data. If information is improperly stored, transmitted, or exposed through an AI application, privacy violations may occur.

Therefore, the adoption of GenAI in digital pharmacy requires more than technical implementation. It requires a governance approach that combines cybersecurity, privacy, professional oversight, risk management, and responsible AI principles.

This research examines the cybersecurity risks associated with GenAI in digital pharmacy services and discusses governance strategies for managing these risks.

GENERATIVE AI IN DIGITAL PHARMACY SERVICES

Generative AI can be applied to several areas of pharmacy management and service delivery.

One important application is patient communication. AI-based conversational systems can provide general medication information, explain terminology, assist with frequently asked questions, and direct patients toward appropriate professional services.

Another application is pharmaceutical documentation. GenAI can assist pharmacists in preparing summaries, reports, educational materials, and administrative documents. This can reduce repetitive documentation work and allow professionals to focus on more complex activities.

GenAI can also support medication information retrieval. Pharmacy professionals may use natural-language interfaces to search large collections of pharmaceutical information. Instead of manually reviewing numerous documents, users can interact with AI systems using conversational questions.

In pharmaceutical research**,** generative models can assist with literature summarization, knowledge discovery, scientific writing support, and hypothesis development. However, generated information must be verified against reliable scientific sources.

GenAI may also support digital pharmacy customer service by handling routine inquiries and providing information about order status, pharmacy services, operating procedures, and general medication-related questions.

Despite these benefits, GenAI should not be treated as an autonomous replacement for qualified pharmacists or healthcare professionals. Its role should primarily involve assistance, information support, and automation of appropriate low-risk activities under suitable controls.

LITERATURE REVIEW

The development of generative AI has attracted substantial interest because large language models can perform a wide range of natural-language tasks. These models can summarize information, answer questions, generate text, translate content, and support knowledge-intensive activities.

Research on AI in healthcare has identified potential benefits in areas such as clinical decision support, medical documentation, patient communication, and healthcare administration. However, researchers have also emphasized the importance of accuracy, explainability, privacy, and human oversight.

Cybersecurity research has identified several emerging risks associated with large language models. Prompt injection is one important concern in which malicious instructions are designed to influence model behavior. Such attacks can become more serious when AI systems are connected to external databases, APIs, or enterprise applications.

Another concern is sensitive information disclosure. AI applications may receive confidential information as part of user prompts or system context. Improper data handling can expose sensitive information.

AI hallucination is also a significant issue. Generative systems may generate plausible but incorrect information. In pharmaceutical environments, incorrect information about medications, dosage, interactions, or contraindications can create serious risks.

The literature therefore indicates that GenAI adoption requires governance mechanisms that address both conventional cybersecurity threats and AI-specific risks.

RESEARCH GAP

Existing studies have examined AI in healthcare and cybersecurity independently, while fewer conceptual studies specifically examine the intersection of Generative AI, cybersecurity, and digital pharmacy services**.**

Most conventional cybersecurity frameworks focus on protecting databases, networks, applications, and user accounts. GenAI introduces additional risks at the model and interaction levels. These include prompt injection, hallucination, malicious content generation, model manipulation, and inappropriate disclosure of information.

Another gap concerns the governance of AI-generated pharmacy information. A conventional cybersecurity system may successfully protect a database from unauthorized access but cannot determine whether an AI-generated medication explanation is clinically accurate.

Therefore, digital pharmacy requires a broader governance model that addresses security, privacy, accuracy, accountability, and human supervision simultaneously**.**

RESEARCH OBJECTIVES

The main objectives of this study are:

- To identify emerging cybersecurity risks associated with Generative AI in digital pharmacy services.
- To examine the potential applications of GenAI in pharmacy environments.
- To analyze privacy and information-security concerns associated with GenAI.
- To propose governance measures for responsible GenAI implementation.
- To examine the importance of human oversight in AI-supported pharmacy services.
- To identify future research directions for secure GenAI adoption in pharmacy.

METHODOLOGY

This research uses a conceptual and literature-based methodology. Existing academic research and established cybersecurity concepts related to Generative AI, healthcare information systems, pharmacy technology, privacy, and AI governance are synthesized to identify emerging risks.

The analysis is organized around four major dimensions: GenAI applications, cybersecurity threats, potential impacts, and governance responses**.**

First, common applications of GenAI in digital pharmacy are identified. Second, cybersecurity risks associated with these applications are analyzed. Third, the potential consequences of these risks for patients, pharmacists, and pharmacy organizations are considered. Finally, governance mechanisms are proposed for reducing these risks.

The study does not use fabricated survey data or experimental performance values. Instead, it provides a conceptual foundation that can be empirically evaluated in future research.

CYBERSECURITY RISKS OF GENERATIVE AI IN DIGITAL PHARMACY

Prompt Injection

Prompt injection occurs when malicious instructions are designed to manipulate the behavior of a generative AI system.

For example, an attacker may attempt to make a pharmacy chatbot ignore its original instructions and reveal information that it should not disclose. If the AI system is connected to internal pharmacy databases, the consequences could be more serious.

Strong system-level controls, input filtering, permission restrictions, and separation between user instructions and sensitive system operations can reduce this risk.

Sensitive Data Disclosure

Digital pharmacy systems may process patient names, medication histories, prescriptions, insurance information, and other sensitive information.

If such information is entered into an improperly controlled AI application, it may create privacy risks. Organizations should therefore establish clear policies regarding what information can be provided to GenAI systems.

Data minimization should be applied so that AI systems receive only the information necessary to perform a specific task.

AI Hallucination

Generative AI can generate incorrect information while presenting it in a confident and convincing manner.

In pharmacy services, hallucinated information can be particularly problematic. Incorrect explanations of medication use, interactions, or safety precautions could mislead users.

Therefore, AI-generated medical or pharmaceutical information should be validated against authoritative sources before being presented as reliable information.

Unauthorized Access

If a GenAI system is connected to pharmacy applications, unauthorized access to the AI interface could potentially provide access to sensitive information or functions.

Role-based access control and multi-factor authentication should therefore be implemented.

Model Manipulation

Attackers may attempt to influence the behavior of an AI system by manipulating training data, knowledge sources, system prompts, or external information.

Organizations should maintain secure model-development and deployment processes and monitor changes to AI systems.

Malicious AI-Generated Content

Generative AI can be misused to create phishing emails, fraudulent messages, fake documents, and social-engineering content.

Pharmacy employees may therefore face increasingly sophisticated phishing attacks. Employee awareness and AI-assisted email security can help reduce this risk.

Insecure API Integration

GenAI applications are often integrated with databases, pharmacy management software, websites, and external services through APIs.

Poorly secured APIs can become attack points. Organizations should implement authentication, authorization, encryption, input validation, and monitoring for AI-related integrations.

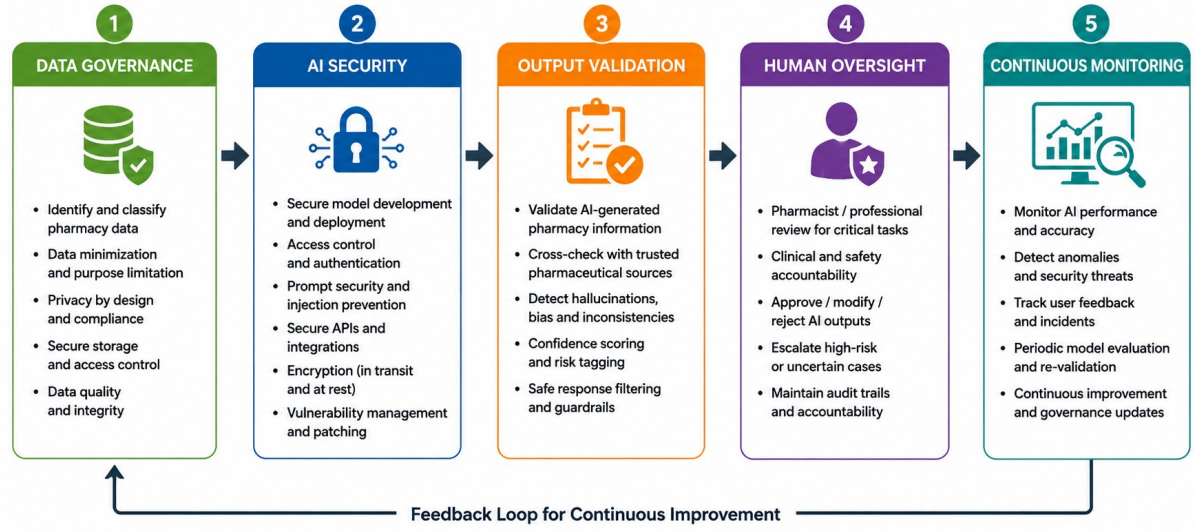
Third-Party and Supply-Chain Risks

Pharmacies may use AI models and services provided by external vendors. Vulnerabilities in third-party platforms, libraries, models, or cloud services may create additional security risks.

Organizations should conduct appropriate vendor assessments and continuously evaluate third-party security practices.

PROPOSED GOVERNANCE MODEL

A responsible GenAI governance model for digital pharmacy can be organized into five major layers:



Data Governance

Organizations should define what pharmacy and patient information can be processed by GenAI systems. Sensitive data should be minimized, protected, and handled according to applicable privacy requirements.

AI Security

AI models and applications should be protected through authentication, authorization, secure APIs, encryption, monitoring, and secure deployment practices.

Output Validation

AI-generated pharmacy information should be checked before being used for high-risk purposes. Information related to medication safety should be validated against trusted sources.

Human Oversight

Qualified pharmacy professionals should remain responsible for decisions involving patient-specific medication management. GenAI should assist rather than independently make high-risk clinical decisions.

Continuous Monitoring

Organizations should continuously monitor AI applications for unusual behavior, security incidents, inaccurate outputs, privacy violations, and changes in system performance.

RESULTS AND DISCUSSION

The conceptual analysis demonstrates that GenAI can provide significant benefits to digital pharmacy services, but its adoption creates a new category of cybersecurity and governance challenges.

The first major finding is that AI security and traditional cybersecurity must be treated together**.** Protecting pharmacy databases and networks is not sufficient when a generative AI application can interact with users and external systems. Security controls must extend to prompts, model behavior, APIs, training data, knowledge sources, and AI-generated outputs.

The second finding is that accuracy represents a security concern in digital pharmacy. Traditional cybersecurity generally focuses on confidentiality, integrity, and availability. In AI-enabled pharmacy services, correctness of generated information is also important. A technically secure AI application can still create risks if it provides incorrect medication-related information.

The third finding is that human oversight remains essential. GenAI can improve efficiency, but it should not independently determine high-risk medication decisions. Pharmacists and healthcare professionals should review AI-generated information where patient safety could be affected.

The fourth finding is that data governance is central to responsible AI adoption. Pharmacy organizations should establish policies defining which information can be processed by AI systems. Data minimization and appropriate privacy controls can reduce unnecessary exposure.

Another finding is that GenAI creates both defensive and offensive cybersecurity possibilities. Organizations can use AI to improve security monitoring, threat intelligence, employee training, and phishing detection. At the same time, attackers can use generative models to create more convincing phishing messages and social-engineering attacks. This creates an evolving cybersecurity environment.

The study also indicates that governance should be treated as a continuous process rather than a one-time activity. AI models, threats, regulations, applications, and organizational requirements change over time. Continuous monitoring and periodic risk assessments are therefore necessary.

PRACTICAL IMPLICATIONS

Pharmacy organizations planning to implement GenAI should begin with low-risk applications such as administrative assistance, general information retrieval, documentation support, and customer-service automation.

Before implementation, organizations should conduct an AI risk assessment. The assessment should consider the type of information processed, system access requirements, potential patient impact, third-party dependencies, and cybersecurity risks.

Employees should receive AI literacy and cybersecurity training. They should understand that AI-generated information may not always be accurate and should know how to identify suspicious AI behavior or phishing attempts.

Organizations should also establish clear accountability. Every AI application should have an identified owner responsible for security, performance, privacy, and compliance.

FUTURE SCOPE

Future research can examine GenAI cybersecurity in pharmacy using real-world datasets and controlled experiments. Researchers can evaluate the effectiveness of different techniques for detecting prompt injection, data leakage, malicious inputs, and hallucinated pharmaceutical information.

Another important area is the development of pharmacy-specific large language models trained and evaluated using reliable pharmaceutical knowledge sources. Such models could potentially reduce hallucination risks when compared with general-purpose systems, although extensive validation would still be required.

Future studies can also investigate privacy-preserving GenAI architectures that minimize the exposure of patient information. Federated learning, secure computation, and privacy-enhancing technologies could be explored for pharmaceutical applications.

The integration of GenAI with pharmacy management systems is another important research area. Future research should examine how AI agents can interact securely with electronic prescriptions, inventory systems, patient communication platforms, and pharmaceutical databases.

Research into AI governance frameworks specifically designed for pharmacies would also be valuable. Such frameworks could combine cybersecurity, privacy, clinical safety, accountability, transparency, and regulatory requirements.

CONCLUSION

Generative AI represents an important technological development for digital pharmacy services. Its ability to understand natural-language queries and generate useful content creates opportunities for improving patient communication, pharmaceutical information management, documentation, research support, and administrative efficiency.

However, the adoption of GenAI introduces cybersecurity risks that differ from those associated with conventional digital systems. Prompt injection, sensitive data disclosure, hallucination, unauthorized access, model manipulation, insecure API integration, malicious AI-generated content, and third-party risks require careful consideration.

The research demonstrates that cybersecurity in GenAI-enabled pharmacy cannot be limited to network protection or database security. Organizations must also protect AI models, prompts, knowledge sources, integrations, and generated outputs. Equally important is the establishment of appropriate governance mechanisms that ensure privacy, accuracy, accountability, and human oversight.

GenAI should therefore be viewed as an assistive technology rather than an independent authority in high-risk pharmacy decisions**.** Its successful adoption depends on the combination of technological safeguards, professional judgment, employee awareness, data governance, continuous monitoring, and responsible AI policies.

Ultimately, the secure adoption of Generative AI can help digital pharmacies improve efficiency and accessibility while maintaining the trust and safety required in healthcare. The future of digital pharmacy will depend not only on how effectively organizations use GenAI, but also on how responsibly they manage its cybersecurity and governance challenges.

REFERENCES

1. *Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big?* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, *610–623*.
2. *Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., et al. (2021). On the opportunities and risks of foundation models.* arXiv preprint arXiv:2108.07258.
3. *Todupunuri, A. (2024). Develop machine learning models to predict customer lifetime value for banking customers, helping banks optimize services. International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, 1(5), 275-282.*
4. *Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends.* Technology and Health Care, 25*(1), 1–10*.
5. *Moor, M., Banerjee, O., Abad, Z. S. H., Krumholz, H. M., Leskovec, J., Topol, E. J., & Rajpurkar, P. (2023). Foundation models for generalist medical artificial intelligence.* Nature, 616, *259–265*.
6. *Singhal, K., Azizi, S., Tu, T., Mahdavi, S. S., Wei, J., Chung, H. W., et al. (2023). Large language models encode clinical knowledge.* Nature, 620, *172–180*.
7. *Weidinger, L., Mellor, J., Rauker, T., Griffin, C., Uesato, J., Huang, P. S., et al. (2022). Taxonomy of risks posed by language models.* Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, *214–229*.
8. *Narapareddy, V. S. R., & Yerramilli, S. K. (2022). Scaling the service now CMDB for distributed infrastructures. International Journal of Engineering Technology Research & Management (IJETRM), 6(10), 101-113.*
9. *Bhagwat, V. B. (2024). A simplified transition from EBS Payroll to Cloud Payroll: Benefits and Drawbacks. Journal of Computational Analysis and Applications, 33(6), 463-474.*
10. *Bhagwat, V. B. (2025). Simplifying Payroll Balance Conversions in Payroll Systems Implementation through the Use of Generative AI.*
11. *Prodduturi, S. M. K. (2025). Efficient Debugging Methods And Tools For Ios Applications Using Xcode. International Journal of Data Science and IoT Management System, 4(4), 1-6.*
12. *Todupunuri, A. (2025). Improving Customer Experience With Modern Banking Solutions. SSRN Electronic Journal. https://doi. org/10.2139/ssrn, 5120615.*