IJCNP, Volume 3, Issue 12, 2025 ISSN: 2995-536X
https://medicaljournals.eu/index.php/IJCNP

INTERNATIONAL JOURNAL OF COGNITIVE NEUROSCIENCE AND PSYCHOLOGY

ENSURING PATIENT DATA CONFIDENTIALITY IN PHARMACY INFORMATION SYSTEMS: ANALYSIS OF CYBERSECURITY THREATS

Turdimuratov Baxtiyor Kurbonovich
Tashkent State Dental University, Termiz Branch Lecturer, Department of Social and Humanitarian Sciences, E-mail: baxtiyor.turdimurodov6668@gmail.com

Rizoqulova Mahliyo Khushvaqt qizi
Tashkent State Dental University, Termiz Branch Faculty of Pediatrics, Pharmacy Department Student, E-mail: mahliyorizoqulova175@gmail.com

Abstract: This article examines cybersecurity threats affecting the confidentiality of patient data in pharmacy information systems. Vulnerabilities in modern e-prescription platforms, pharmaceutical databases, and pharmacy management software are analyzed. Findings show that encryption, authentication, security auditing, and cybersecurity training for employees play a critical role in protecting patient information. The recommendations proposed in this study contribute to strengthening information security.

Keywords: pharmacy information system, patient data, confidentiality, cybersecurity, electronic prescription, encryption.

Introduction

The rapid digitalization of the healthcare system, including pharmacy operations, has created new opportunities. Electronic prescriptions, drug circulation monitoring, automated sales systems, and online pharmacy services provide convenience for patients. However, as patient information is processed in a digital environment, its confidentiality remains highly vulnerable from a cybersecurity perspective.

Medical and pharmaceutical data hold significant value for cybercriminals and are sold at high prices on illegal markets. Since pharmacy information systems are often operated by small enterprises, their cyber defense mechanisms may be weaker compared to large healthcare organizations.

Therefore, scientific analysis of patient data security in pharmacy information systems, assessment of existing threats, and development of effective solutions are essential and relevant.

Research Methods

Theoretical Analysis

International cybersecurity standards (HIPAA, GDPR, ISO/IEC 27001)

Technical architecture of pharmacy information systems

Electronic prescription processing mechanisms

Comparative Analysis

Security measures used in pharmacy systems were compared with those implemented in other healthcare institutions.

Threat Modeling

Cybersecurity threats were classified based on the STRIDE model:

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Expert Survey

A survey was conducted among pharmacists and IT specialists to identify typical vulnerabilities and security issues in pharmacy systems.

Results

Identified Vulnerabilities

Research revealed several key factors threatening patient data confidentiality in pharmacy information systems:

Reuse of passwords and weak password practices

Unencrypted storage of patient databases

Lack of proper authentication mechanisms in API integrations

Unsecured Wi-Fi networks

Untimely system updates (patch management issues)

Common Cybersecurity Threats in Pharmacies

Phishing attacks – employees unknowingly disclose login credentials

Ransomware – data becomes locked and ransom is demanded

Insider threats – unauthorized copying of information by employees

Unauthorized distribution of customer data – illegal sales to insurance companies

Survey Findings

According to survey results:

82% of specialists consider regular data backup the most effective protection method

74% emphasize the necessity of two-factor authentication

68% confirm that cybersecurity training for employees is beneficial

Discussion

Research findings indicate that the cybersecurity level in pharmacy information systems is lower compared to other healthcare segments. This is primarily because pharmacies are small enterprises and allocate limited budgets for IT security.

Lack of encryption, weak passwords, absence of antivirus protection, and insecure network connections significantly increase the risk of data leakage. Ransomware attacks, which have become widespread globally, pose a particularly serious threat to pharmacies.

The study confirms that the following measures are essential for pharmacy information security:

Encryption and secure data transmission (AES, TLS)

Implementation of two-factor authentication

Deployment of properly configured firewalls and EDR systems

Regular staff training

Internal audit and continuous monitoring

Securing API integrations

These measures contribute not only to data confidentiality but also to improving service quality and customer trust.

Digital technologies are now deeply integrated into all levels of the healthcare system, and pharmacy operations depend increasingly on information systems. Pharmacy information systems (PIS) automate processes such as prescription recording, drug circulation control, financial operations, and storage of personal customer information. However, insufficient cybersecurity measures in these systems lead to significant risks.

1. The Importance of Cybersecurity in Pharmacy Information Systems

Information handled in pharmacies includes:

Personal data of customers

Electronic prescriptions

Payment information

Supply chain data of pharmaceuticals

2. Main Types of Cyber Threats

Phishing attacks

Malware and ransomware

Insider misuse of information

Unauthorized database access

Exploitation of network vulnerabilities

3. Importance of International Standards

Compliance with the following standards is crucial for strengthening PIS security:

ISO/IEC 27001

HIPAA

GDPR

4. Ways to Improve Cybersecurity Levels

Strong authentication (2FA/MFA)

Data encryption (AES, TLS)

Regular system updates

Employee training

Data backups

Enhanced network security

Conclusion

Enhancing cybersecurity in pharmacy information systems requires a combination of technical and organizational measures. Encryption, auditing, training programs, and compliance with international standards ensure the protection of patient data.

The study demonstrates that patient data confidentiality in pharmacy information systems remains insufficiently protected. The most serious risks involve malware, phishing, insider threats, and API vulnerabilities. The technical and organizational security measures proposed in this article can significantly improve data protection. Implementing international standards such as ISO/IEC 27001 and HIPAA ensures long-term operational stability for pharmacies.

References

1. ISO/IEC 27001 Information Security Management Standards.
2. HIPAA Security Rule, USA Health System.
3. GDPR General Data Protection Regulation, EU.
4. Smith J. Cybersecurity in Pharmaceutical Information Systems. Journal of Health IT, 2022.
5. Brown P. Data Protection in Digital Pharmacies. International Journal of Pharmacy Tech, 2021.