Farmacia Hospitalaria 48 (2024) T195–T197

Farmacia HOSPITALARIA
Órgano oficial de expresión científica de la Sociedad Española de Farmacia Hospitalaria
www.elsevier.es/farmaciahospitalaria

Editorial

[Translated article] Cybersecurity: a priority for pharmacy services in the age of artificial intelligence

Ciberseguridad, una prioridad de los servicios de farmacia en la era de la inteligencia artificial

In the digital era, hospitals are at a crossroads: on the one hand, the adoption of cutting-edge technologies has revolutionised healthcare, improving accuracy of diagnoses, treatment efficiency, and patients' quality of life. On the other hand, digitalisation has opened the door to increasingly sophisticated cyber threats, endangering sensitive patient data, continuity of care, and even people's lives[1].

As a result, health information is becoming increasingly valuable as well as sought-after. A clear example of this trend is the entry of large corporations, traditionally active in other sectors, into the healthcare sector, along with the creation of dedicated healthcare divisions that are steadily increasing their revenue.

For this reason, cybersecurity has become a progressively important and worrying issue in the healthcare setting. We have experienced significant attacks that have seriously disrupted hospital information systems and thus the delivery of essential healthcare services. A recent study conducted in the United States found that the frequency, sophistication, and duration of cyberattacks on healthcare institutions are increasing[2].

Hospitals are usually prepared to deal with one-off incidents that affect specific systems for a limited period of time. However, cyberattacks can affect all systems and data hosted on the hospital's servers and may persist for extended periods. Cyberattacks are typically planned over weeks or months. These attacks are the most dangerous because they infect backup systems and data long before the attack is detected and action can be taken[3].

The importance of cybersecurity in pharmacy services

Hospital pharmacy services (HPS) face significant challenges in the event of a cyberattack, requiring the identification of key roles and standardised procedures to mitigate the effects of such security breaches. These services play a crucial role in assessing the affected systems and the impact on them, in estimating the duration of downtime, and in planning recovery times to best maintain the medication workflow[4].

Some of the main effects of a cyberattack on HPSs include the following[4]:

- Disruption of critical systems: loss of access to electronic medical records, admission systems, HPS management systems, electronic prescribing and clinical decision support tools, medication administration records, automated dispensing cabinets, dispensing software, and so on.
- Increased manual work: the disruption of automation makes it necessary to carry out activities manually, which can be time-consuming and pose safety risks due to the increased likelihood of errors.
- Impact on productivity and efficiency: the lack of functional systems hinders the availability of information and slows down the process of validating medical orders, which must be performed manually. This also affects the response time for medication delivery and the pharmacotherapeutic follow-up of patients.
- Inventory management challenges: lists must be created manually, and coordination with suppliers for delivery to HPSs is required.
- Communication problems: the disruption of everyday communication systems (e-mail, telephones, messaging apps, etc) can delay the transmission of critical information.
- Documentation and record-keeping issues: the need to manually document medical orders increases the risk of errors and omissions, which can affect the quality of patient care.
- Reorganisation of the work team: close collaboration between pharmacy, medical, nursing, administrative, and other services and departments is required, along with the redeployment of staff and adaptation to new responsibilities and temporary procedures.

In the event of a cyberattack, multidisciplinary collaboration is essential to ensure effective medication management in hospitals and safe pharmaceutical care for patients. To this end, HPSs should establish detailed, up-to-date protocols and develop contingency plans to mitigate risks and maintain high-quality patient care[4,5]. In addition, regular self-assessments of cybersecurity risks should be conducted, as well as drills to ensure that teams are always prepared to respond to potential attacks[6]. Although it is not feasible to conduct drills that simulate real attacks, a schedule of exercises could be established to simulate scenarios with a lower and therefore, more manageable level of impact.

Cybersecurity in the age of Artificial Intelligence

In the world of healthcare, as in virtually all sectors, the adoption of artificial intelligence (AI) is having a huge impact, with significant implications (both positive and negative) for cybersecurity.

https://doi.org/10.1016/j.farma.2024.08.009

The positive impact of AI is diverse and significant:

- It enables the detection of sophisticated threats through predictive analytics, analysing patterns of behaviour and anticipating them before they occur. It also improves the ability to respond quickly to threats in real time, reducing the impact of attacks.
- Without the need for human intervention, it facilitates the automation of security tasks, including continuous monitoring, permanent surveillance of systems and networks, and the identification of anomalies and suspicious behaviour.
- It automates security incidents management, including threat identification, classification, and mitigation.
- Big data analytics. AI can handle and analyse data generated by healthcare systems, identifying patterns and trends that may signal security breaches. It also has the ability to correlate events from multiple sources, providing a holistic view of security.
- It contributes significantly to improved data protection. Algorithms can be used to develop more robust encryption techniques to protect sensitive information. In addition, AI enhances the security of authentication and authorisation systems by using biometrics and behavioural analysis, thereby ensuring a higher level of security.

However, the adoption of AI also poses significant risks and challenges, including the risk of becoming dependent on AI itself. Algorithms are not infallible and can make mistakes in identifying threats, which could result in false positives or false negatives. In addition, the effectiveness of these algorithms depends on the training data. If this data is biased, the AI systems themselves could develop biases, thus affecting their accuracy and effectiveness.

Another challenge is the risk of cyberattacks specifically targeting AI systems. Attackers can manipulate data to deceive AI systems, preventing them from correctly detecting threats (adversarial attacks). If attackers discover vulnerabilities in AI systems, they can exploit them to infiltrate healthcare systems.

Privacy is also a critical issue. To be effective, AI requires access to vast amounts of data, which increases the risk of compromising sensitive data. It is crucial to comply with data protection regulations, which can be complex in the field of AI[7].

Another challenge is that AI systems must be constantly maintained and upgraded to adapt to new threats, which involves additional resources and costs. Furthermore, highly trained personnel are required to manage and operate AI systems, which can be a challenge for many healthcare organisations.

Finally, it is vital that these systems are transparent and that their decisions can be explained and understood by healthcare professionals and security managers. Users need to be confident that AI systems will protect their data and not compromise their privacy[8].

To address these challenges and risks associated with implementing AI in healthcare cybersecurity, comprehensive and rigorous strategies must be adopted. These include continuous risk assessment and conducting regular assessments to identify and mitigate potential vulnerabilities in systems. It is essential to conduct penetration tests and simulated attacks to assess the effectiveness of AI systems and strengthen defences against potential threats. In addition, algorithms should be regularly updated to adapt to new threats and minimise the risk of vulnerabilities being exploited. Establishing a continuous monitoring system to detect and respond to anomalies and threats in real time fulfils the need for constant vigilance[9].

Moreover, continuous training should be provided on the capabilities and limitations of AI systems, as well as on good cybersecurity practices. This includes fostering threat awareness, informing users about threats and their impact on healthcare systems, and promoting a culture of security[7,8].

Finally, the importance of compliance and collaboration cannot be overstated. We must ensure that all systems and processes comply with applicable privacy and security regulations, as well as collaborate with other institutions and regulatory bodies to share threat information and best practices, thereby strengthening our collective defences against cyberattacks[7].

By implementing these strategies, healthcare organisations can significantly improve the security of their AI systems and better protect sensitive patient data.

CRediT authorship contribution statement

Cayetano M. Hernández Marín: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Data curation, Conceptualization. **Emilio Monte-Boquet:** Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Data curation, Conceptualization. **José Luis Poveda Andrés:** Validation, Supervision.

References

1. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: review (for the non-cyber professional). Front Digit Health. 2022;4, 862221. doi: 10.3389/fdgth.2022.862221.
2. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum. 2022;3(12), e224873. doi: 10.1001/jamahealthforum.2022.4873.
3. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A national survey of hospital cyber attack emergency operation preparedness. Disaster Med Public Health Prep. 2023;17(e363):1–4. doi: 10.1017/dmp.2022.283.
4. Santalo O, Perez G, Lorich C, Greenberg M, Hernandez JM, Bohorquez R, et al. Defining key pharmacist and technician roles in response to a hospital downtime or cyberattack. J Am Pharm Assoc. 2023;62(5):1518–23. doi: 10.1016/j.japh.2022.03.027.
5. Alanazi AT. Clinicians' Perspectives on healthcare cybersecurity and cyber threats. Cureus. 2023;15(10), e47026. doi: 10.7759/cureus.47026.
6. Burke W, Stranieri A, Oseni T, Gondal I. The need for cybersecurity self-evaluation in healthcare. BMC Med Inform Decis Mak. 2024;24:133. doi: 10.1186/s12911-024-02551-x.
7. Esmaeilzadeh P. Challenges and strategies for wide-scale artificial intelligence (AI) deployment in healthcare practices: a perspective for healthcare organizations. Artif Intell Med. 2024;151, 102861. doi: 10.1016/j.artmed.2024.102861.
8. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors. 2021;21(15):5119. doi: 10.3390/s21155119.
9. Bhagat SV, Kanyal D. Navigating the future: the transformative impact of artificial intelligence on hospital management – a comprehensive review. Cureus. 2024;16(2), e54518. doi: 10.7759/cureus.54518.

Cayetano M. Hernández Marín[a]
[a]Subdirección de Sistemas de Información, Hospital Universitario y Politécnico La Fe, Valencia, Spain

Emilio Monte-Boquet[b]*
[b]Servicio de Farmacia, Hospital Universitario y Politécnico La Fe, Valencia, Spain

*Corresponding author.
E-mail address: monte_emi@gva.es

José Luis Poveda Andrés[c]
[c]Dirección, Hospital Universitario y Politécnico La Fe, Valencia, Spain