Kelvin Open Science Publishers
Connect with Research Community

Research Article Volume 1 | Issue 1

KOS Journal of AIML, Data Science, and Robotics
https://kelvinpublishers.com/journals/aiml-data-science-robotics.php

Securing AI Chatbots for Medicaid Services: Architecture, Security, and Best Practices

Anand Laxman Mhatre

Senior Program Manager Accenture, State of Texas Austin, TX, USA

*Corresponding author: Anand Laxman Mhatre, Senior Program Manager Accenture, State of Texas Austin, TX, USA

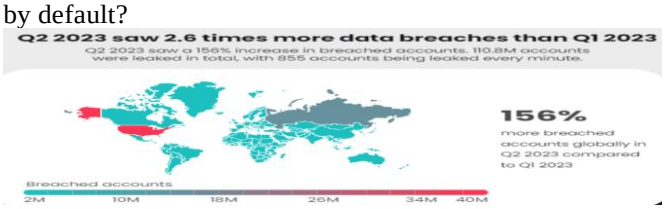
Received: May 09, 2025; **Accepted:** May 21, 2025; **Published:** May 23, 2025

Citation: Anand LM. (2025) Securing AI Chatbots for Medicaid Services: Architecture, Security, and Best Practices. *KOS J AIML, Data Sci, Robot.* 1(1): 1-3.

1. Abstract
Although chatbots are state-of-the-art technologies that enhance user engagement and reduce operational costs, recent evidence suggests that cybercriminals are exploiting them as conduits for accessing company networks and protected data. This document discusses mechanisms and strategies that can be employed to protect Medicaid chatbots.

2. Keywords
Chatbots, Medicaid, Artificial intelligence, Healthcare, Technology

3. Introduction
Chatbots are a novel technology that is revolutionizing patients' engagement in Medicaid services. Today, patients do not have to wait for hours or days to have their inquiries addressed. These technologies can respond to patients in real time, 24/7. Besides responding to inquiries, these tools can send follow-ups and reminders, ensuring adherence to therapy plans. Besides automating communications, they free up human resources, allowing them to focus on more valuable roles. Although chatbots facilitate efficiency in patient engagement, are they secure by default?



4. Chatbots safety
AI chatbots are usually integrated with Medicaid systems and often collect vast quantities of patients' sensitive information. This makes them ideal targets for cybercriminals. According to a report by the World Economic Forum, there is a growing tendency of cybercriminals targeting AI chatbots. The agency observes that as AI chatbots proliferate the commercial and public sectors, the global cybersecurity risk is worsening [1]. For instance, Q2 2023 saw a 156 percent increase in breached accounts. This surge coincided with ChatGPT's popularity growth. Which was launched towards the end of 2022.

Chatbots are ideal targets for cybercrime because they tend to have exclusive access to sensitive information, they are often designed with minimal security layers, their security weaknesses are difficult to spot and fix, and their behavior is constantly evolving, making it easier to introduce security gaps that traditional monitoring tools might miss. Besides, chatbots operate on sophisticated AI models that can be manipulated through adversarial inputs. It is also important to note that chatbots are meant for public use, making them ideal interfaces for launching cyberattacks [2].

5. Chatbot attacks

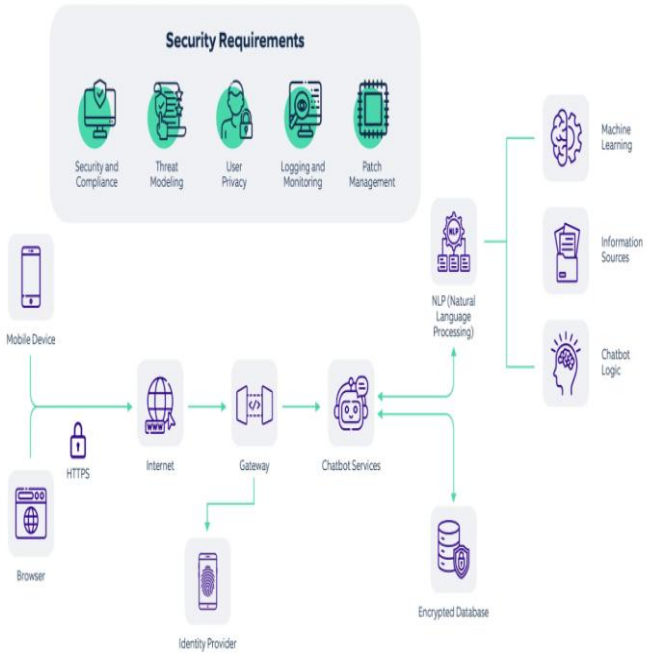
Some of the most common cyberattacks targeting chatbots include;

- ***Prompt injection attacks***: This is a technique where malicious inputs are injected into models to manipulate their behavior and cause them to reveal sensitive information or perform unintended actions. This technique is usually orchestrated on chatbots based on large language models (LLMs). Prompt injection attacks exploit chatbots' lack of contextual behavior.
- ***DoS and bot overload attacks***: chatbots can be a target for denial of service attacks, where malicious bots overload them with requests to degrade their performance and cause outages. A DoS attack on a Medicaid chatbot can render legitimate users unable to access services.
- ***Supply chain attacks***: Usually, chatbots depend on third-party models, libraries, and hosting, that may have vulnerabilities. There is always the risk of attackers exploiting these vulnerabilities to access Medicaid networks and steal data.

6. Securing Chatbots

- Like typical information technology infrastructures, chatbots can be secured by implementing security at multiple layers and leveraging various best practices in the cybersecurity field. Here are various strategies for securing chatbots at different levels.
- ***Secure Architecture***

  Users interact with chatbots via a mobile applications or browsers. While users can interact with generic information without authentication, it is mandatory they verify their identities before accessing sensitive data. It is essential all sensitive information is stored in an encrypted database. The architecture should comprise a gateway for determining data accessible to different users. The diagram below demonstrates the architecture of a secure chatbot.



7. Security

Implementation of security in chatbots should start right from the planning stage to the use training and awareness stage. Here are the key stages for implementing security in chatbots.

- ***Initial phase***: It entails identifying the security needs of the proposed AI chatbot. It is also essential that security objectives be determined prior to the development of the chatbot [3].
- ***Design and architecture***: Security elements should be included in the design of the chatbot's architecture. This phase involves threat modeling – which consists of understanding the system's architecture, identifying potential attack vectors, and then developing countermeasures to protect the chatbot.
- ***Development and coding***: This entails developing security features in the chatbot. This phase also entails observing security-oriented coding practices and conducting code reviews. Static analysis is vital for ensuring the code is secure and works as intended.
- ***Testing***: Once development is complete, the chatbot should be tested to identify unaddressed security issues. Penetration testing and vulnerability scanning are two vital tests that should be conducted.
- ***Deployment***: The servers, databases, and application settings must be configured accordingly to ensure the security of the chatbot. Also, the networks must be configured securely, and firewalls must be integrated strategically into the networks.
- ***Monitoring and incident response***: After deployment, regular security audits and compliance checks should be conducted. It is noble to have an incident response plan ready. This will enable the security team to respond swiftly to security threats.
- ***Updates and patches***: Regularly updating the chatbot to stay ahead of emerging threats.
- ***User training and awareness***: It is important to train users on best security practices and social engineering threats. Users should be advised on the type of data they can feed into chatbots.

8. Best Practices

The security of Medicaid chatbots can be further enhanced by developers and security teams leveraging the following best practices.

- ***Leveraging OWASP Top 10 principles for LLM***: OWASP's Top 10 principles provide clear guidelines on how to handle user inputs, manage data, understand potential risks and vulnerabilities, and take appropriate steps for mitigation. It is a rule of thumb to incorporate these principles when building a chatbot.
- ***Implement access privileges***: Give users different privileges, preventing unauthorized access to sensitive data and administrative functions.
- ***Input validation***: Sanitize user inputs to prevent attacks such as SQL injection or cross-site scripting (XSS) attacks.
- ***Limited data collection access***: The chatbot should only have access to necessary data. It should not prompt users to provide unnecessary data.
- ***Rate limiting and CAPTCHA***: Use these strategies to combat brute-force attacks and DoS attacks.
- ***Self-destructive messages***: This strategy is effective for preventing the exposure of sensitive data in instances of unauthorized access.

9. Conclusion

As chatbots are integrated with Medicaid systems, cybercriminals will attempt to use them as attack surfaces for accessing patients' sensitive data. Unfortunately, contemporary chatbot architectures and models are not designed with security at their cores. As CMS integrates

chatbots in Medicaid services, it must take necessary steps to ensure that developed chatbots are equipped with essential security measures. This document has highlighted some of the best strategies that can be exploited to build and deploy secure Medicaid chatbots.

10. References

1. World Economic Forum. (2024) Prompt injection attacks threaten AI chatbots, and other cybersecurity news to know this month.
2. Costa AF, Coelho NM. (2024) Evolving Cybersecurity Challenges in the Age of AI-Powered Chatbots: A Comprehensive Review. In: *Doctoral Conference on Computing, Electrical and Industrial Systems*. Cham: Springer Nature Switzerland. 217-228.
3. Nagarro. (2023) Building secure chatbots: Best practices that ensure privacy.