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

Modernizing Medicaid IT: Cybersecurity Compliance, Cybersecurity Requirements, and Zero Trust Architecture

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 20, 2025; **Published:** May 22, 2025

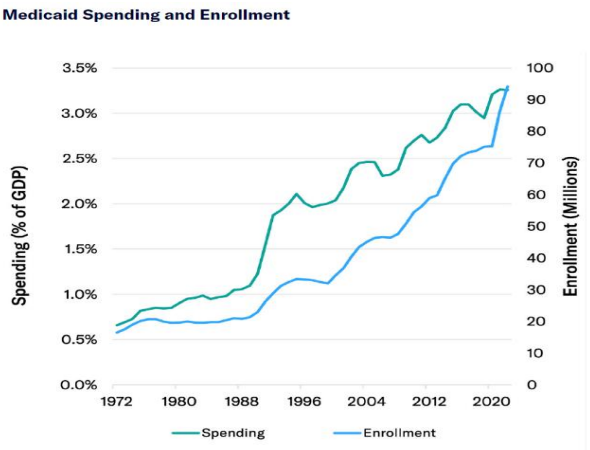
Citation: Anand LM. (2025) Modernizing Medicaid IT: Cybersecurity Compliance, Cybersecurity Requirements, and Zero Trust Architecture. *KOS J AIML, Data Sci, Robot.* 1(1): 1-3.

1. Abstract
The Medicaid program serves close to 90 million people and receives funding of about 3.5 percent of the GDP. To handle this large number of users and efficiently manage and administer allocated funds, Medicaid systems must be secure and compliant with healthcare data privacy regulations. This document discusses cybersecurity regulations that apply to Medicaid IT systems, and explores requirements and frameworks necessary for ensuring safety and compliance of these systems.

2. Keywords
Medicaid, IT systems, modernization, cybersecurity, compliance, zero trust architecture

3. Introduction
Since its inception, the Medicaid program has been expanding as the US population grows and laws permit more people to access it. According to the Manhattan Institute, Medicaid membership grew from less than 20 million in 1972 to more than 90 million in 2020. The institute also asserts that Medicaid spending increased from less than 1 percent of the GDP in 1972 to close to 3.5 percent of the GDP in 2020 [1]. KFF asserts that although Medicaid enrollment has declined in recent years, the spending is still growing, and enrollment is expected to surge in future [2].

As Medicaid membership grows and the government allocates more funds to the program, its IT systems must be modernized to augment their capacity, mitigate cyber threats, and enhance efficiency. Besides, these systems must be updated regularly to remain at par with the changing regulatory landscape and shifting internal requirements.



3. Regulatory landscape
Medicaid IT systems hold personally identifiable information (PII) and protected health information (PHI) of over 80 million Americans. Like all other electronic systems that hold

critical patient data, Medicaid systems must comply with various cybersecurity regulations. These regulations include;

3.1. HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a federal regulation designed to safeguard electronic protected health information (ePHI) stored in IT systems. It sets the standards of how PHI can be used and disclosed, and mechanisms that must be installed to prevent disclosure or unauthorized access of patients' data. Keys aspects of HIPAA that apply to Medicaid IT systems include;

- ***Privacy rule***: Medicaid systems must limit access to patients' data, only allowing use/disclosure for permitted functions like treatments, payments, and known operations.
- ***Administrative safeguards***: System administrators must develop and enforce security policies and procedures, conduct regular risk assessments, and assign security responsibility to specific personnel.
- ***Physical safeguards***: Install measures to secure systems' physical facilities such as servers and mobile devices.
- ***Technical safeguards***: Medicaid systems must have access control mechanisms. These systems must also have extra security features such as data encryption and regular audit controls to track access to protected data.
- ***Breach notification***: In cases where Medicaid systems are breached and over 500 records are disclosed, HHS must be informed. The regulation also directs that members whose records are breached must be briefed.

3.2. HITECH Act (Health Information Technology for Economic and Clinical Health Act)

The primary goal of the HITECH Act is to encourage widespread adoption and meaningful use of technology in healthcare to improve healthcare quality, data security, and patient care efficiency. The regulation reinforces the HIPAA regulation by enabling implementation of HIPAA requirements. Key aspects of the HITECH Act applicable to the Medicaid IT systems are;

- **Incentive program:** The Act authorized funding for improving and modernizing Medicaid IT systems to adhere to HIPAA. It also incentivized eligible professionals and hospitals serving Medicaid patients to upgrade their IT systems.
- **Penalties:** Increased penalties for HIPAA non-compliance.
- **Breach notification requirements:** Expanded breach notification requirements, including the requirement for reporting breaches to media outlets.
- **Document HIPAA compliance:** The act directed CMS and providers serving Medicaid patients to document their HIPAA compliance.

3.3. 21st Century cures act

The law was ratified to accelerate the development of infrastructure for sharing healthcare information. The act directs healthcare IT infrastructures, such as Medicaid systems, to create networks that facilitate interoperability in the healthcare sector. The act emphasizes protection against information blocking while maintaining strong privacy protections. It mandates Medicaid systems to facilitate secure access and exchange of health data.

Regulation	Requirements
HIPAA	Risk analysis
	Access controls
	Data encryption
	Monitoring
	Oversight
	Incidence response and reporting
HITECH Act	Incentives
	Interoperability
	HIPAA reinforcement
Century Cures Act	Interoperability
	Secure data transfer

4. Medicaid IT systems cybersecurity requirements

While cybersecurity regulations like HIPAA provide the basis for developing secure healthcare IT infrastructures, more is required to develop an absolute secure system. Besides the aforementioned regulations, there are additional requirements for safeguarding Medicaid IT systems. They include;

- ***Security Frameworks***: Incorporating security frameworks such as NIST Cybersecurity Framework and MITA 3.0 is essential for enhancing patients' records safety. NIST Cybersecurity Framework's five core functions - identify, protect, detect, respond, and recover - are vital for improving security and incident response. On the other hand, MITA 3.0 integrates security standards in Medicaid modernization.
- ***Risk assessments and incident management***: Throughout the system's lifetime, periodic risk assessments should be conducted to identify vulnerabilities and threats [3]. A formal incident response plan should be maintained.
- ***Secure system design and operations***: The system's overall architecture must be informed by potential security threats. Data encryption should be enforced on data both at rest and in transit. Third-party components must be assessed to ensure they comply with security requirements. The systems should be patched and updated regularly.
- ***Cloud security***: Cloud providers should comply with FedRAMP. Interoperability should be implemented via secure APIs. Security assessments should be conducted on all modules involved in cloud computing infrastructure.
- ***Governance and Training***: Medicaid IT systems must have a dedicated security governance team. Medicaid staff working with IT systems must be trained regularly on cybersecurity and HIPAA compliance.

5. Zero Trust Architecture

Zero Trust Architecture, commonly abbreviated as ZTA, is a security model that treats all devices inside and outside the network as suspicious, and must continuously be verified to continue accessing network resources. It deviates from traditional perimeter-based security to identity-centric approach. The model is suitable for Medicaid IT infrastructure because of the sensitivity of these systems' data and their vulnerability to sophisticated cyberattacks. Also, ZTA is apt for Medicaid's distributed IT infrastructure. ZTA attributes that make it ideal for Medicaid IT systems include;

- **Least privilege:** ZTA is strictly designed to enforce least privileges to users and devices. This attribute is essential for minimizing the severity of potential attacks.
- **Continuous verification:** ZTA is designed to continuously verify devices and users whenever they request access to resources in the network. This ensures ultimate network safety.
- **Microsegmentation:** The architecture segments the networks into mini-isolated networks, restraining the spread of attacks in networks in case of breaches.
- **Breach inevitability:** ZTA assumes that networks such as Medicaid systems will eventually be breached regardless of the installed security measures. The framework is designed to anticipate and contain attacks.
- **Enhanced compliance:** Besides its safety features, ZTA provides an architecture readily compliant with most data privacy regulations. Medicaid IT systems that incorporate ZTA have fewer difficulties corresponding to privacy regulations.

6. Conclusion

Cybersecurity is a core element of Medicaid IT modernization. Modern Medicaid IT systems must be secure and compliant with data privacy regulations such as HIPAA, HITECH, and all government directives. This document has explored the essential requirements of a modern, secure Medicaid IT system and proposed Zero Trust Architecture and other frameworks like NIST as the fundamental building blocks for creating safe, modernized Medicaid IT systems.

7. References

1. Manhattan Institute. (2024) Slowing Optional Medicaid Spending Growth.
2. KFF. (2024) Medicaid Enrollment & Spending Growth: FY 2024 & 2025.
3. Halsey MN. (2022) A Cybersecurity Assessment of Health Data Ecosystems.