REPORT HIGHLIGHTS

October 2025 | A-18-24-00002

Summary Report of Prior Office of Inspector General Penetration Tests of 10 State MMIS and E&E Systems

Why OIG Did This Audit

- In the health care sector, State Medicaid Management Information Systems (MMIS) and Eligibility & Enrollment (E&E) systems are increasingly targeted by cybercriminals because of the valuable sensitive information they contain. There has been a noticeable increase in ransomware, phishing, and denial-of-service attacks that pose significant risks to critical health care systems and the data they manage.
- Between 2020 and 2022, OIG conducted penetration tests on 10 State MMIS and E&E systems. These tests were designed to simulate cyberattacks to evaluate how effectively these systems were protected against such threats.

What OIG Found

Overall, we found that:

- the 10 States implemented generally effective information technology security controls for their web-facing MMIS and E&E systems to prevent unsophisticated or limited cyberattacks, but they need to continue to improve these controls to prevent more sophisticated and persistent cyberattacks;
- cyber attackers would likely need a moderate to significant level of sophistication or complexity to compromise the State systems we audited; and
- the 10 States effectively detected and responded to some of our simulated cyberattacks but they need to improve their detection and response to other types of cyberattacks.

What OIG Recommends

This summary report contains no recommendations to the Centers for Medicare & Medicaid Services (CMS); however, it does provide an overview of the recommendations previously made to the 10 States.

CMS informed us that it did not have comments on our draft report.