REPORT HIGHLIGHTS

July 2025 | A-18-22-08019

A Large Northeastern Hospital Could Improve Certain Security Controls for Preventing and Detecting Cyberattacks

Why OIG Did This Audit

- Health care's growing reliance on information technology for patient care, telemedicine, and records has heightened vulnerability to cyberattacks. HHS has an important role in guiding and supporting the adoption of cybersecurity measures to protect patients and health care delivery from cyberattacks.
- This audit examined whether a large hospital in the northeast United States (referred to as the "Entity") had implemented cybersecurity controls to (1) prevent and detect cyberattacks, (2) ensure continuity of patient care in the event of a cyberattack, and (3) protect Medicare enrollee data.

What OIG Found

The Entity implemented cybersecurity controls to ensure continuity of patient care in the event of a cyberattack and protect Medicare enrollee data. However, it could improve specific cybersecurity controls to better prevent and detect cyberattacks. We found:

- Among the 26 internet-accessible systems analyzed, 2 had weaknesses in their cybersecurity controls that could allow unauthorized user access.
- 13 web applications and 16 internet-accessible systems had weaknesses in their cybersecurity controls, making them susceptible to interactions and manipulations by attackers.

What OIG Recommends

We made five recommendations to the Entity to improve its cybersecurity measures, including that it enforce configuration management policies, assess and update authentication controls, assess and update configuration management controls, conduct regular assessments of internet accessible systems for vulnerabilities, and ensure that developers follow secure coding practices. The full recommendations are in the report.

The Entity concurred with all five of our recommendations.