REPORT HIGHLIGHTS

January 2026 | A-18-22-08021

A Large Southeastern Hospital Could Improve Certain Security Controls to Enhance Its Ability to Prevent and Detect 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 southeast 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 protect against cyberattacks, ensure the continuity of patient care in the event of a cyberattack, and protect Medicare enrollee data. However, the Entity could improve specific cybersecurity controls to further strengthen its defenses against cyberattacks. Among the four internet-accessible web applications analyzed, our testing showed that:

- An account management web application had a cybersecurity control weakness related to access. Specifically, the web application lacked strong user identification and authentication controls, such as multi-factor authentication. As a result, we were able to use login credentials captured from our phishing campaign to gain account management access.
- An internet-facing web application had a cybersecurity control weakness related to system and information integrity. Specifically, the web application lacked strong data input validation controls and did not employ adequate protections —such as a web application firewall— to detect and block web-based attacks. As a result, the application may have been susceptible to injection attacks, including the insertion of malicious code by threat actors.

What OIG Recommends

We made four recommendations to the Entity to improve its cybersecurity controls by strengthening its practices for safeguarding the Entity's systems, including internet-accessible websites and applications from cyberattacks. The full recommendations are in the report.

The Entity concurred with all four of our recommendations.