# REPORT HIGHLIGHTS

June 2026 | OAS-25-18-033

# A Small Southeastern Hospital Had Effective Cybersecurity Controls To Prevent, Detect, and Respond To Cyberattacks

## Why OIG Did This Audit

- The health care sector's growing reliance on information technology for patient care, telemedicine, and records has heightened vulnerability to cyberattacks. HHS plays an important role in guiding and supporting the adoption of cybersecurity measures to protect sensitive patient data and health care delivery from cyberattacks.

- This audit examined whether a small hospital in the southeast United States (the Entity) had implemented cybersecurity controls to prevent, detect, and respond to cyberattacks.

## What OIG Found

The Entity implemented effective cybersecurity controls to prevent, detect, and respond to cyberattacks, including our simulated cyberattacks. The controls included a custom system designed to block unusual or suspicious activity. The Entity detected and flagged our testing as suspicious, indicating operational monitoring and responsiveness to potential threats.

## What OIG Recommends

This report does not contain recommendations.