Department of Health and Human Services
Office of Inspector General
Office of Audit Services

June 2026 | OAS-25-18-033

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

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.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

Health care organizations, including hospitals, have increasingly relied on information technology (IT) systems for patient care, telemedicine, and records management. However, this reliance has made them vulnerable to cyberattacks, including ransomware incidents and sophisticated attacks aimed at compromising medical records. The Department of Health and Human Services (HHS) provides cybersecurity guidance, oversight, and outreach to health care organizations. HHS' Office for Civil Rights (OCR) maintains a public website called the Breach Portal, which tracks large health data breaches.[1] According to the site's data, the number of patient records affected by these breaches grew from 6 million in 2010 to 170 million in 2024. During that period, hacking and IT-related incidents increased from 2 percent of all breaches in 2010 to 91 percent in 2024. In total, 732 million patient records were affected between 2010 and 2024, with 88 percent of those attributed to hacking or IT issues.[2]

732 million patient records were affected by data breaches between 2010 and 2024.

88% were attributed to **hacking** or IT-related issues.

The growing number of cyberattacks against health care organizations raises questions about whether HHS, including the Centers for Medicare & Medicaid Services (CMS), could strengthen its cybersecurity guidance, oversight, and outreach to help these organizations implement more effective cybersecurity controls. This audit is one in a series of HHS Office of Inspector General (OIG) audits of hospitals' cybersecurity controls.[3, 4] The auditee was a small hospital in the southeast United States (hereinafter referred to as the "Entity") that participates in the Medicare and Medicaid programs. Because of the threat of cyberattacks against the health care sector, we are not identifying the Entity.

---

[1] The Breach Portal tracks data breaches that affect 500 or more people, as required by federal law under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology of Economic and Clinical Health Act.

[2] John Xuefeng Jiang, Joseph S. Ross, Ge Bai, "Ransomware Attacks and Data Breaches in US Health Care Systems," *The Journal of the American Medical Association Network Open*, vol. 8, no. 5, (May 14, 2025). Accessed on Feb. 20, 2026.

[3] OIG, *A Large Northeastern Hospital Could Improve Certain Security Controls for Preventing and Detecting Cyberattacks* (A-18-22-08019), July 2, 2025.

[4] OIG, *A Large Southeastern Hospital Could Improve Certain Security Controls to Enhance Its Ability to Prevent and Detect Cyberattacks* (A-18-22-08021), Jan. 30, 2026.

OBJECTIVE

Our objective was to determine whether the Entity had implemented cybersecurity controls to prevent, detect, and respond to cyberattacks.

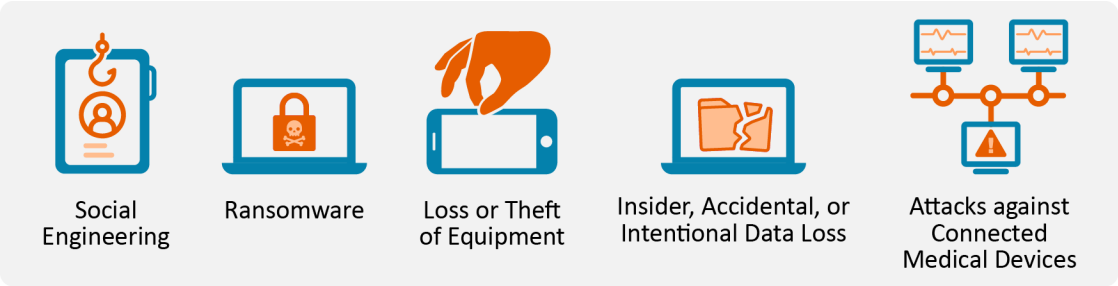
BACKGROUND

The Threat to Health Care and the Public Health Sector

The health care sector is a prime target for cybercriminals seeking to exploit vulnerabilities for financial gain or to disrupt critical medical services. Balancing innovation and efficiency in health care while also enhancing its defenses against cyber threats remains a challenge for the health care sector. Further, the absence of a required, unified, and robust cybersecurity framework across the health care sector may expose certain entities to potential attacks, risking the compromise of sensitive patient data and patient safety.

The Cybersecurity Act of 2015, section 405(d), "Aligning Health Care Industry Security Approaches," established voluntary guidelines for cybersecurity in the health care industry. HHS, in collaboration with various stakeholders, developed the HHS 405(d) Task Group, which identified the top five threats facing the health care sector (see Figure 1).[5]

Figure 1: Top Five Threats Facing Health Care and Public Health Sector



The variety of regulations and cybersecurity best practices, along with differences in how they are implemented within the health care sector, makes it challenging for the Federal Government to implement a comprehensive and standardized approach to safeguarding health care systems.[6]

In October 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency, the Federal Bureau of Investigation, and HHS issued an advisory regarding

[5] HHS 405(d) Task Group, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (2023 Edition)*. Accessed on Dec. 17, 2025.

[6] HHS, "Security Rule Guidance Material." Accessed on Dec. 17, 2025.

imminent ransomware attack activity targeting the health care sector. The advisory stated that those agencies had credible information of an increased and imminent cybercrime threat to U.S. entities and warned health care providers to take timely and reasonable precautions to protect their networks from those threats.

HHS tracks large data breaches through OCR, whose data showed a 93 percent increase in large breaches from 2018 to 2022 (369 to 712), with a 278 percent increase in large breaches involving ransomware from 2018 to 2022.[7]

The Entity

The Entity is a small hospital in the southeastern United States with fewer than 50 beds and offers various health services, including stroke rehabilitation, neurological condition treatment, and orthopedic condition treatment.[8] The Entity is part of a network of providers that share protected health information for treatment, payment, and health care operations. The Entity adopted the National Institute of Standards and Technology (NIST) *Cybersecurity Framework* (CSF) 2.0 as its main cybersecurity control framework. The CSF provides guidance to organizations of all sizes and sectors for managing cybersecurity risk. It defines high-level cybersecurity outcomes to help organizations understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it references resources and practices that can be used to achieve those outcomes. This document maps the CSF to controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* and other regulatory requirements. We used NIST SP 800-53, Revision 5, as the Informative Reference for this audit.

Federal Requirements

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which is found in subpart C of 45 CFR part 164, describes the administrative, physical, and technical safeguards required to ensure the confidentiality, integrity, and availability of electronic protected health information and protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information.

CMS developed the Conditions of Participation (CoPs) that hospitals must meet to participate in the Medicare and Medicaid programs. The CoPs require hospitals to comply with regulations and standards to protect patient information, maintain the integrity of their IT systems, and ensure compliance in areas that overlap with the HIPAA Security Rule. The HIPAA Security Rule

[7] HHS, *Healthcare Sector Cybersecurity, Introduction to the Strategy of the U.S. Department of Health and Human Services.* Accessed on Dec. 17, 2025.

[8] According to HHS 405(d) Task Group guidance cited in *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (2023 Edition), entities with fewer than 50 beds are considered small. Accessed on Dec. 17, 2025.

mandates specific security standards while allowing flexibility so that entities can choose reasonable and appropriate security measures.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, includes controls that provide government and non-government organizations with a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets. By implementing the controls, organizations can establish a robust security posture that meets cybersecurity standards and aligns with cybersecurity best practices, ensuring the confidentiality, integrity, and availability of their data.

HOW WE CONDUCTED THIS AUDIT

We reviewed the Entity's policies and procedures in effect during our testing to assess cybersecurity practices related to contingency planning and incident response.[9] We also conducted interviews with Entity officials to gain further insights into the Entity's cybersecurity practices and risk mitigation strategies.

To assist us with evaluating the Entity's IT cybersecurity controls, we contracted with BreakPoint Labs, LLC (BPL) to provide subject matter experts who conducted penetration testing of the Entity's internet-accessible systems, web application testing, and vulnerability scanning and analysis. We conducted penetration testing that focused on four of the Entity's websites, in accordance with the Rules of Engagement (ROE) document signed by OIG, BPL, and the Entity. We focused on both public internet protocol (IP) addresses and web application URLs, as specified within the ROE document. Testing took place in June 2025.[10]

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our results and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our results and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology, and Appendix B contains the Federal requirements, Entity-adopted cybersecurity framework, and Federal cybersecurity guidelines we used to evaluate the Entity's cybersecurity controls.

RESULTS OF AUDIT

The Entity's cybersecurity controls in place during our audit successfully detected our testing as suspicious and prevented our cyberattacks. The controls included a custom system designed to

[9] We used HHS 405(d) Task Group cybersecurity practices for small healthcare organizations for our assessment.

[10] We note that the testing we performed may not have disclosed all IT control deficiencies that existed at the time of this audit.

block unusual or suspicious activity. The testing results indicate operational monitoring and responsiveness to potential threats.

THE ENTITY IMPLEMENTED CYBERSECURITY CONTROLS TO PREVENT, DETECT, AND RESPOND TO CYBERATTACKS

During our audit, we observed that the Entity had adopted NIST CSF 2.0 and implemented measures to prevent and detect cyberattacks. These measures included a defense-in-depth network architecture, documented incident response procedures, and contingency planning controls designed to maintain continuity of operations. Below are the results of our testing and review of these controls.

The Entity Prevented and Detected Our Simulated Cyberattacks

The Entity had a defense-in-depth network architecture with effective cybersecurity protections in place, including a custom system designed to block unusual or suspicious activity.[11] During the audit, the Entity promptly identified and flagged our penetration testing as suspicious.

The penetration test identified a low-risk issue involving certain systems that did not enforce a secure transport setting.[12] However, the Entity had already recognized this issue before our testing and had formally accepted the associated risk. The Entity is also working with a vendor to explore options for reducing the risk over the long-term.

The Entity was able to prevent and detect our simulated cyberattacks against the selected public-facing websites, demonstrating an effective threat prevention and detection capability that contributes to the protection of sensitive data and critical services.

Incident Response Controls Implemented To Respond to Cyberattacks

The Entity had documented policies and procedures for incident response that comply with NIST SP 800-53's Incident Response control requirements, such as training, testing, and handling. To meet these requirements, the Entity conducted annual comprehensive cybersecurity training, routine vulnerability scanning, continuous monitoring, and regular tabletop training exercises. The Entity also conducted annual third-party penetration testing to evaluate and strengthen its response capabilities.

The Entity's efforts demonstrated an operational incident response process that supports timely detection, analysis, containment, and recovery from security incidents. These practices

[11] Defense-in-depth is a cybersecurity strategy that uses multiple security products and practices across multiple control layers—physical, technical, and administrative—to safeguard an organization's network, web properties, and resources.

[12] Secure transport settings refer to configurations that ensure secure communication between applications over a network.

enhance the Entity's ability to maintain continuity of care and protect critical systems in the event of a cyberattack.

Contingency Planning Controls Implemented To Respond to Cyberattacks

The Entity documented and implemented contingency plan policies and procedures aligned with NIST SP 800-53's Contingency Planning control requirements. It conducted and tracked its contingency training as part of its emergency management education program, with both initial and ongoing training tailored to individual roles and responsibilities. The Entity tested its contingency plan twice a year and updated it annually based on risk assessments.

Backup and disaster recovery policies and procedures were documented. Procedures included nightly backups, which are replicated to an off-site disaster recovery location and tested at least monthly to ensure data integrity and recoverability. Based on documentation and interviews, backup workstations allowed access to clinical data during system outages, and disaster recovery exercises were conducted quarterly to validate technical readiness. Data were encrypted at rest and in transit to ensure confidentiality and integrity.

As a result, the Entity was positioned to respond to disruptive events—such as natural disasters or cyberattacks—and recover critical systems and data in a timely manner. This backup and recovery capability supports continuity of operations, minimizes service interruptions, and helps safeguard patient care and sensitive information.

CONCLUSION

The Entity successfully detected and prevented our simulated cyberattacks on the systems tested. The implementation of a defense-in-depth network architecture and the establishment of regular leadership meetings focused on emerging threats, security strategies, and ongoing improvements to cybersecurity practices demonstrated the Entity's commitment to effective cybersecurity.

On the basis of these results, we are not making recommendations to the Entity.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

Our audit included an assessment of select IT general controls and application controls for the Entity's systems we assessed. We assessed the Entity's cybersecurity policies and procedures in effect at the time of our testing to assess controls related to contingency planning and incident response. We also conducted interviews with Entity officials to gain further insights into the Entity's cybersecurity practices.

We conducted penetration testing that focused on four of the Entity's websites, in accordance with the ROE document agreed on and signed by OIG, BPL, and the Entity. We focused on both public IP addresses and web application URLs, as specified within the agreed-on ROE document. The testing we performed may not have disclosed all IT control deficiencies that existed at the time of this audit.

We conducted our audit work from January 2025 through April 2026. The penetration testing took place in June 2025.

METHODOLOGY

To assist us with evaluating the Entity's cybersecurity controls, we relied on the work of specialists. We contracted with BPL to provide subject matter experts. BPL testing included conducting external penetration testing, web application testing, and vulnerability scanning and analysis of the Entity's internet-accessible systems. OIG oversaw the work to ensure that all objectives were met, and that testing was performed in accordance with government auditing standards and the ROE document. Our testing methodology focused on network or infrastructure that supported selected internet-accessible applications, application program interfaces, websites, web applications, and other external resources.

In June 2025, we began gathering information and confirming the network addresses supporting selected IT systems. We performed penetration testing to determine whether internet-accessible systems were susceptible to exploits by a threat actor.

We reviewed Federal requirements for covered entities under HIPAA, NIST SP 800-53, Revision 5 controls, and industry cybersecurity best practices to determine whether the Entity's controls aligned with cybersecurity standards and industry best practices.

In addition, we evaluated the Entity's contingency planning and incident response practices by examining policies, training records, risk assessments, and system documentation. We verified that the Entity had implemented policies and procedures for the backup process and contingency plan testing, including disaster recovery, and that they were aligned with Federal requirements. We confirmed that data were encrypted and accessible during outages through

tested backup systems. We also conducted interviews with Entity's officials to understand the controls in place.

Prior to the issuance of our draft report, we provided the Entity with detailed documentation outlining our preliminary results. We provided the Entity with a draft report on April 22, 2026, for review. The Entity elected not to provide formal comments.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our results and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our results and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS AND FEDERAL CYBERSECURITY GUIDELINES

FEDERAL REQUIREMENTS

Health Insurance Portability and Accountability Act Security Rule

According to 45 CFR § 164.306 (Security standards: General Rules):

> (c) Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in §§ 164.308 [Administrative safeguards], 164.310 [Physical safeguards], 164.312 [Technical safeguards], 164.314 [Organizational requirements] and 164.316 [Policies and procedures and documentation requirements] with respect to all electronic protected health information.

CMS Conditions of Participation

According to 42 CFR § 482.1 (Basis and Scope), hospitals participating in Medicare must meet specific standards set forth by the program. Additionally, the Secretary has the authority to impose further requirements if deemed necessary to protect the health and safety of individuals receiving services in these hospitals.

According to 42 CFR § 482.24 (Condition of participation: Medical record services), the hospital must maintain a medical record for each inpatient and outpatient. Medical records must be accurately written, promptly completed, properly filed and retained, and accessible. The hospital must use a system of author identification and record maintenance that ensures the integrity of the authentification and protects the security of all record entries. Medical records must be retained in their original or legally reproduced form for a period of at least 5 years.

The *State Operations Manual's Appendix A—Survey Protocol, Regulations, and Interpretive Guidelines for Hospitals* requires hospitals to comply with Federal requirements set forth in the Medicare CoPs to receive Medicare or Medicaid payments. CMS conducts surveys of Hospitals to ensure that they meet minimum requirements in accordance with the Medicare CoPs and CMS's interpretive guidelines.

FEDERAL CYBERSECURITY STANDARDS, GUIDELINES, AND PRACTICES

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

This publication describes a voluntary risk management framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. NIST CSF's prioritized, flexible, and cost-effective approach helps to promote the

protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST CSF includes informative references to certain security controls including NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets from a diverse set of threats and risks.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov