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

January 2026 | A-18-22-08021

A Large Southeastern Hospital Could Improve Certain Security Controls to Enhance Its Ability to Prevent and Detect Cyberattacks

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.

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. In 2022 alone, the Department of Health and Human Services' (HHS's) Office for Civil Rights received reports of 64,592 health care data breaches affecting nearly 42 million health care records that may have been exposed or stolen.[1] HHS provides cybersecurity guidance, oversight, and outreach to health care organizations. The large number of cyberattacks against health care organizations' IT systems raises questions regarding whether HHS, including the Centers for Medicare & Medicaid Services (CMS), can do more with its cybersecurity guidance, oversight, and outreach to help health care organizations implement robust cybersecurity controls to improve their cybersecurity measures. This audit is one in a series of HHS, Office of Inspector General (OIG) audits of hospitals' cybersecurity controls. The auditee was a large hospital in the southeast United States (hereinafter referred to as the "Entity") that participates in the Medicare and Medicaid programs. Due to the threat of cyberattacks against the health care sector, we are not identifying the Entity.

> In 2022 alone, HHS received reports of **64,592** health care data breaches affecting nearly **42 million** health care records that may have been exposed or stolen.

OBJECTIVE

Our objective was to determine whether the Entity had implemented cybersecurity controls to (1) prevent or detect cyberattacks, (2) ensure continuity of patient care in the event of a cyberattack, and (3) protect Medicare enrollee data.

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 simultaneously enhancing its defenses against cyber threats remains a challenging task for the health care sector. Further, the absence of a required, unified, and

[1] Office for Civil Rights, *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022*. Accessed on May 23, 2024.

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 (CSA), 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.)[2]

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.[3]

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

There was a **93%** increase in large breaches reported from 2018 to 2022.

HHS tracks large data breaches through the Office for Civil Rights, whose data show a 93 percent increase in large breaches reported from 2018 to 2022 (369 to 712), with a 278 percent increase in large breaches involving ransomware from 2018 to 2022.[4]

[2] Source: HHS 405(d) Task Group, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. Accessed on Feb. 7, 2024.

[3] HHS, "Security Rule Guidance Material." Available online at https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html. Accessed on Mar. 7, 2024.

[4] HHS, *Healthcare Sector Cybersecurity, Introduction to the Strategy of the U.S. Department of Health and Human Services.* Accessed on Aug. 8, 2025.

The Entity

The Entity is a large hospital in the southeast United States that has more than 300 beds and offers various health services, including emergency, cardiac, neurology, maternity, and radiology services.[5] The Entity is part of a network of providers that share protected health information (PHI) for treatment, payment, and health care operations.[6] The Entity adopted the Health Information Trust Alliance (HITRUST) *Common Security Framework* (CSF), version 9.4, as its main cybersecurity control framework in effect at the time of our testing. The HITRUST CSF is a certifiable framework that provides organizations with a comprehensive approach to regulatory compliance and risk management. The framework maps its controls to standards from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other regulations and standards to help provide a comprehensive and flexible framework tailored to managing the privacy and security of health information. Therefore, we used HITRUST CSF, version 9.4 as our main criteria for this audit.

Federal Requirements

The HIPAA Security Rule, which is found in subparts A and 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 (ePHI) 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 such as the HIPAA Security Rule to protect patient information and maintain the integrity of their IT systems. The HIPAA Security Rule mandates specific security standards while allowing flexibility so that entities can choose reasonable and appropriate security measures to meet these requirements.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, includes controls that provide government and non-government organizations with a comprehensive framework for enhancing their cybersecurity and privacy programs. 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.

[5] HHS 405(d) Task Group guidance to the health care sector defines entities with more than 300 beds as large. See: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Accessed on May 15, 2024.

[6] This arrangement is considered an organized health care arrangement, as defined in 45 CFR § 160.103.

On January 13, 2017, CMS issued a memorandum to State Survey Agency Directors to remind providers and suppliers to keep current with best practices regarding mitigation of cybersecurity attacks. In the memo, CMS also provided resources to assist facilities in their reviews of their cybersecurity and IT programs.[7]

HOW WE CONDUCTED THIS AUDIT

We reviewed the Entity's policies and procedures in effect at the time of our testing to assess cybersecurity practices related to data protection and loss prevention, network management, and incident response.[8] 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 relied on the work of specialists. We contracted with BreakPoint Labs (BPL) to provide subject matter experts to conduct penetration testing of the Entity's internet-accessible systems, web application testing, vulnerability scanning and analysis, and phishing campaigns. Testing took place from August through September 2022.

We conducted penetration testing and external vulnerability assessment on four of the Entity's internet-facing web applications.

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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings 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.

FINDINGS

The Entity implemented cybersecurity controls (e.g., network architecture, backup strategies, incident response, and disaster recovery controls) to ensure continuity of patient care in the event of a cyberattack and protect Medicare enrollee data. Also, the Entity implemented cybersecurity controls that prevented and detected most of our simulated cyberattacks. However, the Entity could improve its cybersecurity controls to better prevent or detect certain types of cyberattacks.

[7] CMS Recommendations to Providers Regarding Cyber Security. Accessed on July 9, 2024.

[8] We used HHS 405(d) Task Group cybersecurity practices for large organizations for our assessment.

We successfully captured a user's login credentials through our email phishing campaign attacks. The captured credentials allowed us to gain access to the Entity's account management web application for the user because the Entity did not design and implement strong user identification and authentication (UIA) controls for the account management web application. Weak UIA controls could allow malicious threat actors to compromise web application authenticators (e.g., username and password) or manipulate the web application's functionality, elevate their privileges within the system, and extract sensitive data from the application database. To our knowledge, the systems we were able to exploit did not contain patient information. However, threat actors could have used the user account information gathered from within the application to perform more targeted social engineering campaigns and attacks to find exploitable weaknesses in critical administrative or clinical systems on the Entity's network.

Additionally, we found that one of the four web applications we tested had a security weakness in its input validation controls that allowed manipulation of the application. The weakness existed because the Entity did not conduct effective testing of the web application to identify vulnerabilities and because the web application was not behind a web application firewall (WAF) to protect it from malicious traffic. Without the effective testing of web applications and effective WAF protection, input validation vulnerabilities in the Entity's other web applications could have been exploited. Such exploitation could lead to the execution of malicious code or manipulation of web applications.

PHISHING CAMPAIGN RESULTS

As part of our email phishing campaign, we sent out 2,171 phishing emails to test whether users would click a link to our fake website and enter their login credentials. Of the 2,171 emails sent, the last 500 emails were blocked. The first 1,671 emails resulted in 108 users (6 percent) clicking the link. One of the users who clicked the link entered their login credentials to our fake website, which we captured and used for other attacks. Due to the low click-rate and login-rate by users, the results of our phishing campaign do not indicate a systemic failure or reportable finding; therefore, we are not making a recommendation related to the phishing campaign. We shared these results as information-only and encouraged the Entity to review its email phishing controls to determine whether any improvements may be helpful.

ONE WEB APPLICATION LACKED STRONG USER IDENTIFICATION AND AUTHENTICATION CONTROLS

HIPAA sets standards for protecting electronic health information, focusing on security and privacy to prevent unauthorized access. Similarly, the HITRUST CSF recommends the use of strong UIA controls when accessing systems with sensitive data. This enhances security for both remote and administrative access. The HITRUST CSF references NIST SP 800-53, which contains security and privacy controls recommended for use by organizations. Key recommendations from NIST include implementing robust UIA controls for access to data. Both

HITRUST and NIST emphasize the importance of combining employee training with technical security measures, such as strong UIA controls to boost overall organizational security.

As described above, we successfully captured a user's login credentials as part of our email phishing campaign attacks. We then used the captured credentials to access the Entity's account management web application for that user. This web application was set up to accept usernames and passwords from users accessing it via the internet. Once we accessed the web application, we were able to view the user's devices associated with their specific account and a list with options to activate or deactivate multi-factor authentication (MFA) and add or remove devices from the user's account.[9]

We were able to use the login credentials we obtained to access the Entity's account management web application because the Entity did not design and implement strong UIA controls (e.g., MFA) into the authentication process for this specific web application. Instead, the Entity relied on other less robust mitigating controls that rely on a manager's approval or authorization from another device to approve changes to the account. However, a skilled bad actor using techniques such as social engineering could defeat the controls to deceive someone into unknowingly approving account changes submitted via the vulnerable account management web application.

If a threat actor were able to compromise an account, they would be able to collect information about the user's devices and account settings that could be used for further attacks. For example, it may be possible for an attacker to delete the registered user's devices in the web application and then use social engineering techniques to set up their own controlled devices that can be used for authenticating to the network. This could allow the attacker to gain access to other Entity applications.

ONE WEB APPLICATION LACKED STRONG INPUT VALIDATION CONTROLS

The HITRUST CSF states that data entered into applications and databases shall be validated to ensure that the data are correct and appropriate. It further states that organizations should ensure that internet-facing web applications are protected against known attacks by installing an automated technical solution, such as a WAF, that detects and prevents web-based attacks. Similarly, NIST 800-53 recommends using input validation controls to ensure accuracy and prevent security threats, such as injection attacks. Further, the HIPAA Security Rule, section 164.306(a), requires covered entities and business associates to safeguard ePHI against any reasonably anticipated threats or hazards to the security and integrity of ePHI.

The Entity did not implement strong data input validation controls for one of its internet-facing web applications, which made that application vulnerable to an injection attack. This type of attack enables a malicious actor to introduce harmful code via weak input fields and alter

[9] Per our agreed-upon Rules of Engagement with the Entity, we did not attempt to change any settings to the user's account.

commands sent to the website. As a result, bad actors can execute unauthorized commands, access sensitive data, or manipulate the system. The Entity stated that the vulnerability existed because a vendor-provided software update introduced the vulnerability to the web. Despite conducting vulnerability scans and third-party penetration tests, the Entity failed to detect the input validation vulnerability in its web application during its security testing process before updating production systems. Additionally, the web application was not protected by a WAF that could filter, monitor, and block malicious web traffic such as injection attacks. After we notified the Entity about the vulnerability, the Entity stated that it fixed the vulnerability as part of a software update and placed the web application behind a WAF for extra protection.

Without properly testing web applications for effective input data validation controls and placing them behind an effective WAF, vulnerabilities like ineffective input validation can be exploited by threat actors to execute malicious code or manipulate web applications. For example, a threat actor could exploit weak input validation controls in a web application and use it to upload and host malware that can be spread to the other computers visiting the web application.

RECOMMENDATIONS

We recommend that the Entity:

- implement strong user identification and authentication controls for the account management web application we exploited;

- periodically assess and update user identification and authentication controls across the Entity's systems, including internet-accessible websites and applications;

- assess all web applications to determine whether any need an automated technical solution (e.g., a web-application firewall) implemented as an extra layer of security to detect and block malicious web traffic and attempts to exploit web application vulnerabilities; and

- utilize a wider array of security testing tools and techniques to better detect vulnerabilities in applications before updating production systems, such as dynamic application testing tools, static application testing tools, and manual, interactive testing, as part of its security testing process prior to deploying updates to internet-accessible production systems.

ENTITY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, the Entity concurred with all four of our recommendations and described actions that it has taken and plans to take to address them. Specifically:

- Regarding our first recommendation, the Entity stated that it deploys a "defense in depth" strategy to mitigate compromised user identifications, including risk-based processes such as "step up" authentication to authorize the performance of sensitive functions and actions in applications.

- Regarding our second recommendation, the Entity stated that it continues to review and implement technologies and training that include various multi-factor user authentication technologies to support a zero trust framework. The Entity also assesses its controls against multiple frameworks, including the HITRUST and NIST CSFs, and monitors security assessments for alignment with industry practices to ensure its controls are effective and supported by accepted standards and practices.

- Regarding our third recommendation, the Entity stated that it continues to deploy web application firewalls, vulnerability detection tools, and attack surface management capabilities to supplement a "defense in depth" posture for all web-facing assets.

- Regarding our fourth recommendation, the Entity stated that it continues to review and deploy tools and techniques to: (1) directly integrate static code analysis directly into application development workflows for internally developed web applications, (2) dynamically test both internally and commercially developed applications, and (3) assess and validate internal and external software development life cycle programs. The Entity also stated that it continues to expand appropriate participation in information threat-sharing cooperation to leverage time-sensitive industry awareness.

Although we have not yet confirmed the actions described in the Entity's response, we commend the Entity for its ongoing efforts to improve its overall security posture.

The Entity's comments are included in their entirety as Appendix C.[10]

[10] The Entity opted to not provide its comments on official letterhead and provided its comments as presented.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

Our audit included an assessment of IT general controls and application controls for the Entity's systems we assessed. We assessed the Entity's policies and procedures in effect at the time of our testing to assess cybersecurity practices related to data protection and loss prevention, network management, and incident response. We also conducted interviews with Entity officials to gain further insights into the Entity's cybersecurity practices and risk mitigation strategies.

We conducted penetration testing that focused on 4 of the Entity's web applications, in accordance with the Rules of Engagement (ROE) document agreed upon and signed by OIG, BPL, and the Entity. We focused on both public IP addresses and web application URLs, as specified within the agreed-upon ROE document. We note that 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 June 2022 through October 2025. The penetration testing took place between August and September 2022.

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 phishing campaigns, 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.

We reviewed Federal requirements for covered entities under HIPAA. We also reviewed HITRUST CSF, NIST SP 800-53, Revision 4 controls, and industry cybersecurity best practices to determine whether the Entity's controls aligned with cybersecurity standards and industry cybersecurity best practices. Additionally, we reviewed the Entity's policies and procedures to determine whether it adequately designed and implemented effective cybersecurity controls to prevent, detect, and recover from cyberattacks.

We reviewed the Entity's network architecture, backup strategies, incident response, and disaster recovery controls to determine whether they ensured the continuity of patient care during a cyberattack and protected Medicare enrollee data. Our assessment included technology and tool efficacy in protecting data and networks, the integrity of backup systems across multiple regions, and the implementation of incident response through penetration testing. Additionally, we assessed the Entity's testing of its disaster recovery plans and readiness to ensure it aligned with Federal requirements and best practices. We also conducted interviews with Entity's officials to understand the controls in place.

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 August 2022, 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.

In September 2022, BPL conducted two simulated phishing campaigns to determine whether the Entity had implemented appropriate controls to detect and prevent successful email phishing attacks and to determine whether Entity personnel would recognize and appropriately respond to such emails. The Entity provided a list of the employees who were subjected to BPL's phishing campaigns. The phishing campaigns included a link to a fake website we controlled, which if clicked on, attempted to collect information about the user's web browser and computer device, such as patch level, web browser add-ons, and operating system version.

Prior to the issuance of our draft report, we provided the Entity with detailed documentation outlining our preliminary findings.

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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS, ENTITY ADOPTED 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):

> (a) General requirements. Covered entities and business associates must do the following:
>
> > (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
> >
> > (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
> >
> > (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
> >
> > (4) Ensure compliance with this subpart by its workforce.
>
> (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.

State Operations Manual Appendix A — Survey Protocol, *Regulations, and Interpretive Guidelines for Hospitals* requires Hospitals be in compliance 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.

ENTITY-ADOPTED REQUIREMENTS

HITRUST Common Security Framework Version 9.4.5

01.q User Identification and Authentication:

> All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user.
>
> . . . [A]ppropriate authentication methods including strong authentication methods in addition to passwords are used for communicating through an external, non-organization-controlled network (e.g., the Internet). . .

10.b Input Data Validation:

> Data input to applications and databases shall be validated to ensure that this data is correct and appropriate.
>
> . . . For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
>
> 1. reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes;
>
> 2. installing an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic. . .

FEDERAL CYBERSECURITY GUIDELINES

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal 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. These controls include the following:

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of [Assignment: organization-defined information inputs].

APPENDIX C: ENTITY COMMENTS

A Large Southeastern Hospital Could Strengthen Certain Security Controls to Better Prevent and Detect Cyberattacks

OIG RECOMMENDATIONS & THE ENTITY RESPONSES

We *[the OIG]* recommend that the Entity:

- **implement strong user identification and authentication controls for the account management web application we exploited;**

  ENTITY RESPONSE: The Entity concurs with the recommendation to implement strong user identification and authentication controls for the account management web applications. Entity deploys a "defense in depth" strategy to mitigate compromised user identifications, including risk based processes such as "step up" authentication to authorize the performance of sensitive functions and actions in applications.

- **periodically assess and update user identification and authentication controls across the Entity's systems, including internet-accessible websites and applications;**

  ENTITY RESPONSE: The Entity concurs with the recommendation that a comprehensive information security program should periodically assess and update user identification and authentication controls. The Entity continues to review and implement technologies and training that includes various multi-factor user authentication technologies to support a zero trust framework. The Entity also assesses the Entity's controls against multiple frameworks including HITRUST and NIST CSF and monitor security assessments for alignment with industry practices to ensure the Entity's controls are effective and supported by accepted standards and practices.

- **assess all web applications to determine whether any need an automated technical solution (e.g., a web-application firewall) implemented as an extra layer of security to detect and block malicious web traffic and attempts to exploit web application vulnerabilities; and**

  ENTITY RESPONSE: The Entity concurs with the recommendation that web applications should be assessed to determine whether any additional automated technical solutions are appropriate as an extra layer of security to detect and block malicious web traffic and attempts to exploit web application vulnerabilities. The Entity continues to deploy web application firewalls, vulnerability detection tools, and attack surface management capabilities to supplement a defense in depth posture for all web facing assets.

1

A Large Southeastern Hospital Could Strengthen Certain Security Controls to Better Prevent and Detect Cyberattacks

OIG RECOMMENDATIONS & THE ENTITY RESPONSES

- **utilize a wider array of security testing tools and techniques to better detect vulnerabilities in applications before updating production systems, such as dynamic application testing tools, static application testing tools, and manual, interactive testing, as part of its security testing process prior to deploying updates to internet-accessible production systems.**

  ENTITY RESPONSE: The Entity concurs with the recommendation to utilize a wider array of security testing tools and techniques to better detect vulnerabilities in applications prior to updating production systems to account for the evolving and wide scope of threat actors.

  The Entity continues to review and deploy tools and techniques to: (1) directly integrate static code analysis directly into application development workflows for internally developed web applications; (2) dynamically test both internally and commercially developed applications; and (3) assess and validate internal and external software development life cycle programs. The Entity also continues to expand appropriate participation in information threat sharing cooperation to leverage time sensitive industry awareness.

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