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

July 2025 | A-18-22-08019

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

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.

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 northeast 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

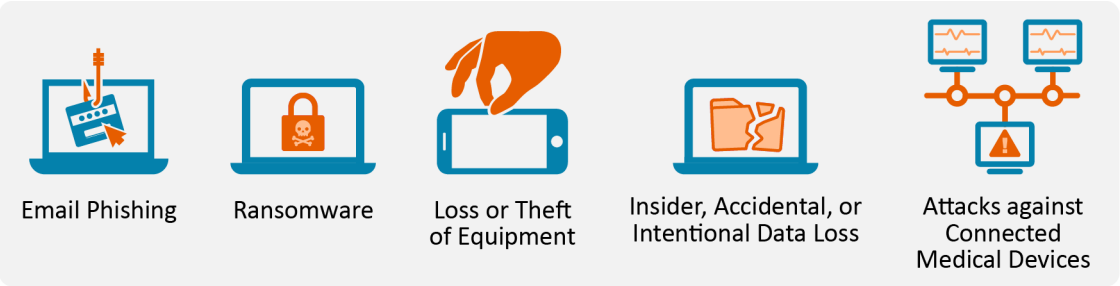
The health care sector is a prime target for cybercriminals seeking to exploit vulnerabilities for financial gain or to disrupt critical medical services. Balancing innovation and efficiency in health care while simultaneously enhancing its defenses against cyber threats remains a challenging task for 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. The Secretary of 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 these 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.

[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.

The Entity

The Entity is a large hospital in the northeast United States that has more than 300 beds and offers various health services, including emergency, cardiac, neurology, maternity, radiology, and trauma services.[4] The Entity is part of a network of providers that share protected health information (PHI) for treatment, payment, and health care operations.[5] The Entity voluntarily adopted the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF).[6] The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices. The Framework is aimed at reducing and better managing cybersecurity risks. NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* is one of six informative references that an organization can follow to achieve NIST CSF Core outcomes. We used NIST SP 800-53, Revision 4, as the informative reference for this audit.

Federal Requirements

The Health Insurance Portability and Accountability Act of 1996 (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 the 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

[4] 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.

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

[6] NIST Cybersecurity Framework V1.1 was the most current version at the time of our audit. Accessed on September 4, 2024.

cybersecurity standards and aligns with cybersecurity best practices, ensuring the confidentiality, integrity, and availability of their data.

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 and web applications, vulnerability scanning and analysis, and phishing campaigns. Testing took place during May 2022.

We conducted penetration testing on 26 of the Entity's internet-accessible systems, including 13 web applications. Additionally, we conducted an external vulnerability assessment that focused on 255 of the Entity's public IP addresses.

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, Federal cybersecurity standards, guidelines, and industry cybersecurity best practices we used to evaluate the Entity's cybersecurity controls.

FINDINGS

The Entity implemented effective 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's

[7] CMS Memorandum to State Survey Agency Directors, S&C: 17-17-All (Jan. 13, 2017).

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

cybersecurity controls were generally effective at preventing and detecting our simulated cyberattacks. However, the Entity could improve its cybersecurity controls to better prevent and detect other types of cyberattacks.

Specifically, the Entity's cybersecurity controls were generally effective at preventing and detecting our simulated cyberattacks against its internet-accessible systems due to its web application firewall (WAF) that limited and blocked our malicious requests. Also, none of the Entity's employees to whom we sent our phishing emails interacted with the fake website we set up for our email phishing attacks. However, we found weaknesses in some of the Entity's web application security controls, including a weakness in the Entity's design and implementation of an identification and authentication control, which allowed us to gain unauthorized access to one of its internet-accessible systems. Additionally, our penetration testing identified 13 web applications that had weaknesses related to configuration management controls. Also, our vulnerability assessment found 16 internet-accessible systems that had weaknesses related to identification and authentication controls, which could allow an attacker to interact with and manipulate the internet-accessible systems. Addressing these weaknesses would improve the overall security of the Entity's internet-accessible systems and applications and prevent certain cyberattacks.

These weaknesses occurred because the entity integrated two systems to its existing IT environment without following certain industry security best practices. Also, the Entity's procedures to periodically assess the security controls implemented on web applications and systems were not effective at identifying weaknesses before they were potentially exploited. In addition, the Entity did not effectively implement industry web application security best practices (e.g., Open Worldwide Application Security Project best practices) for its web applications to minimize the risk of exploitation by bad actors.

As a result, the Entity's systems were susceptible to some of the cyberattacks we conducted. The Entity stated that the systems we were able to exploit did not contain patient information. However, if compromised, the systems could serve as a launch pad for initiating additional attacks against other Entity systems, which may host ePHI. Further, threat actors could use the information gathered from a compromised system to perform more targeted social engineering campaigns and deceive Entity's staff or contractors into providing sensitive information (e.g., system logon credentials) and launch further attacks to find exploitable weaknesses in critical administrative or clinical systems on the hospital network.

TWO SYSTEMS HAD SECURITY WEAKNESSES IN CONTROLS USED TO PREVENT UNAUTHORIZED USER ACCESS

The NIST CSF, adopted by the Entity, offers voluntary standards, guidelines, and practices for healthcare organizations to manage cybersecurity risks. The NIST CSF references security controls from NIST SP 800-53, Revision 4, which are also recommended for non-Federal organizations. Key recommendations include implementing strong identification and authentication controls for remote access, documenting configuration settings for IT products

in a restrictive mode aligned with operational needs and analyzing the security impact of changes to information systems before implementation.

We discovered security vulnerabilities in the identification and authentication and configuration management controls, in 2 of the 26 internet-accessible systems that underwent our penetration testing. Because these systems were accessible over the internet, they were at a higher risk of being targeted and exploited by malicious actors compared to systems that are only accessible from within an organization's private network. In one of the two systems, we identified a way for unauthenticated users to view a list of valid usernames due to a misconfiguration. Using the usernames, we were able to exploit weak identification and authentication controls in the other system to guess the passwords and successfully sign in.[9]

These weaknesses occurred because the entity integrated two systems to its existing IT environment without following certain industry security best practices. Although the Entity had developed a configuration and change management policy requiring security impact analyses be conducted for new or modified systems, it relied on the IT vendor's configuration, which did not include controls needed to prevent the security weaknesses. The Entity clarified that both systems were configured using settings recommended by an IT vendor and were used for project management, and not clinical care.

According to the Entity, the systems that we were able to exploit did not contain ePHI. However, these weak controls posed risks to the Entity's computer network and were not adequate to protect against any reasonably anticipated threats or hazards to the security or integrity of other systems hosting ePHI. For example, the compromised system could have served as a launch pad for attackers to initiate additional cyberattacks against other Entity systems, some of which may store ePHI. Further, the compromised web application accounts could allow threat actors to modify existing webpages or create new ones within the Entity's web application. These altered or newly created pages could then be used to host malware or include links to malicious websites, which could be used as part of social engineering attacks to gain access to sensitive information.

After we notified the Entity of the weaknesses with the two internet-accessible systems, Entity officials stated that they disabled remote access to the two systems and changed the compromised passwords. The Entity also stated that it was working on strengthening its password policy, enhancing its identification and authentication controls, and evaluating other solutions that follow NIST guidelines and security best practices. We have not yet confirmed these changes but plan to review the Entity's remediation efforts during our audit resolution process.

[9] This technique is commonly known as a password spraying attack.

MULTIPLE WEB APPLICATIONS AND SYSTEMS HAD SECURITY WEAKNESSES

The HIPAA Security Rule, Section 164.306(a), requires that covered entities and business associates safeguard ePHI against any reasonably anticipated threats, including cyberattacks on internet-accessible web applications. To mitigate such risks, the NIST SP 800-53, Revision 4, recommends that organizations identify and rectify system flaws, establish stringent configuration settings for IT products, and limit system functionalities to only those that are necessary. Additionally, it advises that feedback from authentication systems should not reveal information that could help unauthorized individuals access authentication details.

During our penetration testing, we assessed 13 web applications and found weaknesses related to configuration management or systems and information integrity controls for all 13 web applications. Specifically, we identified web applications that either (1) were not configured to operate in the most restrictive mode aligned with operational needs or (2) failed to limit information and functions strictly to provide essential capabilities. For example, we identified a vulnerability in one web application that did not limit unnecessary interaction with external systems (e.g., a mail server). This flaw could enable attackers to use the web application to gain access to connected systems to launch attacks on other connected systems.[10] Depending on the Entity's network architecture, this may potentially allow for the exploitation of internal systems or services not otherwise accessible to external attackers. We also identified a different vulnerability in another web application—an attacker could modify certain data sent to the web application and potentially broadcast malicious data to other users visiting the web application.

Further, our external vulnerability assessment found that 16 of the Entity's 255 internet-accessible systems were improperly configured for authenticator feedback. Improper authenticator feedback could allow cyberattackers to discover valid usernames by analyzing error messages received from the Entity's internet-accessible systems. This technique—known as account discovery—is used to facilitate cyberattacks.

The weaknesses occurred because the Entity's procedures for periodically assessing the security controls of web applications and systems were ineffective in identifying and remediating vulnerabilities before they could be exploited. Additionally, the Entity did not effectively apply secure coding best practices—such as those published by the Open Worldwide Application Security Project— when implementing its web application.

We did not identify patient information on the systems we tested. However, the weaknesses such as those we identified could be exploited by threat actors to collect user account information and perform targeted phishing attacks. Also, a skilled attacker might create a malicious computer program and upload it to the Entity's web application, tricking users into running the malicious program and uncovering additional exploitable weaknesses.

[10] This may include public third-party systems, internal systems within the same organization, or services available on the system hosting the web application itself.

RECOMMENDATIONS

We recommend that the Entity:

- enforce and periodically assess compliance with its configuration and change management policy, which requires that a security impact analysis be performed for all newly deployed or modified systems, including contractor-deployed systems, and that any discovered issues or unsecure configuration settings are resolved before a system is deployed or exposed to the internet;

- periodically assess and update its identification and authentication controls in its systems to ensure:

    - users are uniquely identified and authenticated;

    - strong authentication and authenticators (e.g., passwords) have sufficient strength to prevent common cyberattacks against authentication controls (e.g., password spraying); and

    - feedback of authentication information during the authentication process is not disclosed;

- periodically assess and update its configuration management controls in its systems to ensure:

    - information system flaws are identified and timely corrected;

    - configuration settings for IT products on its systems are secure and in compliance with established configuration baselines; and

    - systems functionality, including functions, ports, protocols, and services are limited to only those that are necessary;

- establish a policy or process to periodically assess its internet-accessible systems and applications security controls against security control standards from NIST SP 800-53 or similar industry web application security standards and promptly resolve any identified weaknesses, and

- implement a policy that requires developers to follow secure coding practices for its web applications in accordance with the Entity's approved cybersecurity framework or industry web application security best practices for coding, testing, and maintaining web applications and establish a procedure to confirm adherence to the requirements.

ENTITY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, the Entity concurred with all five 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 conducts periodic security reviews of contractor-deployed solutions and will continue to focus on contractor-deployed systems in its reviews and enforce remediation of any critical issues or misconfigured settings before a system is deployed or exposed to the internet.

- Regarding our second recommendation, the Entity stated that it is evaluating additional solutions to further enhance and strengthen its authentication and security controls, including a solution to detect compromised or breached passwords and require password changes for affected users.

- Regarding our third recommendation, the Entity stated that it will continue to work with application teams and vendors to enforce stricter controls, including compliance with remediation timelines and maintenance of configuration baselines.

- Regarding our fourth recommendation, the Entity stated that it will continue to review its policies, processes, and security controls to ensure they are properly updated to reflect industry best practices and NIST guidelines and will enhance its controls as necessary.

- Regarding our fifth recommendation, the Entity updated its policies to incorporate secure coding practices for internally developed applications using "Security by Design" principles, including input validation, secure error handling, secure data storage, and protection against common security vulnerabilities.

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

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 on 26 of the Entity's internet-accessible systems, including 13 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. Additionally, we conducted an external vulnerability assessment that focused on 255 of the Entity's public IP addresses. 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 January 2022 through April 2025. The penetration testing took place during May 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 IT 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 NIST CSF, NIST SP 800-53, Revision 4 controls, industry cybersecurity best practices, and *Health Industry Cybersecurity Practices* Technical Volume 2 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, and other external resources.

In May 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 May 2022, BPL conducted 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 campaign. 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, STANDARDS, GUIDELINES, AND PRACTICES, AND INDUSTRY CYBERSECURITY BEST PRACTICES

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 for Hospitals

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.

FEDERAL CYBERSECURITY STANDARDS, GUIDELINES, AND PRACTICES

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

This publication describes a voluntary risk management framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. NIST CSFs 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

According to the NIST CSF version 1.1:

Risk Assessment (ID.RA)

ID.RA-1: Asset vulnerabilities are identified and documented.

Identity Management, Authentication and Access Control (PR.AC)

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Information Protection Processes and Procedures (PR.IP)

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)

PR.IP-3: Configuration change control processes are in place

PR.IP-12: A vulnerability management plan is developed and implemented.

Protective Technology (PR.PT)

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

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:

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation

Control Enhancements: (2) SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS
The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

CM-7 LEAST FUNCTIONALITY

Control: The organization:

a. Configures the system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

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).

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

INDUSTRY CYBERSECURITY BEST PRACTICES

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

The *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* examines cybersecurity threats and vulnerabilities that affect the health care industry. It explores 5 current threats and presents 10 practices to mitigate those threats to the health care sector. It is designed to be useful for organizations of all sizes, offering resources and best practices across the main document and two technical volumes. We used *Technical Volume 2 Cybersecurity Practices for Medium and Large Health Care Organizations* to assess this Entity because it discusses the 10 cybersecurity practices for medium and large health care organizations:

2.M.A Basic Endpoint Protection Controls

Hardened Baseline Images — Configure the endpoint operating system in the most secure manner possible.

Disable unnecessary service and programs.

Review and consider the implementation of Security Technical Implementation Guides.[11]

3.M.A Identity

Establish each person's identity through onboarding systems of record. Identities maintain a series of attributes that describe common user elements. The system of record transmits attributes to the IAM system, enriching the identity data and facilitating the flow of information to systems for login, access management, and other cybersecurity- and business-related functions.

3.M.D Multifactor Authentication for Remote Access

MFA should be implemented on remote-access technologies to limit the exposure of password credentials that could be compromised through phishing or malware attacks.

7.M.B: Web Application Scanning – NIST Framework Ref: DE.CM-8

[11] "Security Technical Implementation Guides," Information Assurance Support Environment, available online at https://public.cyber.mil/stigs/. Accessed on Mar. 8, 2024.

> . . . Most web applications run dynamic code, run atop a web server, interact with middleware, and connect to databases. If the web application is not coded securely, this architecture may enable unanticipated access to data or systems. Common web application attack types include Structured Query Language (SQL) injection, cross-site scripting, and security misconfigurations. In these cases, attackers can:
>
> bypass web application security controls and pull data directly from the database, steal an already authenticated cookie on a vulnerable website to get access, exploit misconfigurations that can permit properly formatted commands or scripts to execute privileged content on the webserver itself . . .
>
> . . .In all cases, vulnerabilities to web applications with sensitive information represent a high risk to your organization. It is important to understand these vulnerabilities to conduct appropriate and prioritized remediation.

7.M.D Patch Management, Configuration Management, & Change Management

> [O]rganizations should ensure that proper security configuration management activities are in place.
>
> [In addition], consideration needs to be given to changes made to systems, servers, and networks, along with the vulnerabilities that may be exposed as a result. A testing plan should be part of the change management process.

Open Worldwide Application Security Project Secure Coding Practices Quick Reference Guide

This technology agnostic document defines a set of general software security coding practices, in a checklist format, that can be integrated into the software development lifecycle. Implementation of these practices will mitigate most common software vulnerabilities.

> [28] All authentication controls should fail securely
>
> [33] Authentication failure responses should not indicate which part of the authentication data was incorrect. For example, instead of "Invalid username" or "Invalid password", just use "Invalid username and/or password" for both. Error responses must be truly identical in both display and source code
>
> [38] Enforce password complexity requirements established by policy or regulation. Authentication credentials should be sufficient to withstand attacks

that are typical of the threats in the deployed environment (e.g., requiring the use of alphabetic as well as numeric and/or special characters)

[45] Temporary passwords and links should have a short expiration time

[107] Do not disclose sensitive information in error responses, including system details, session identifiers or account information

[109] Implement generic error messages and use custom error pages

[154] Restrict the web server, process, and service accounts to the least privileges possible

[156] Remove all unnecessary functionality and files

APPENDIX C: ENTITY COMMENTS

DATE: May 16, 2025

TO: Tamara Lilly, Assistant Inspector General for Cybersecurity & Information Technology Audits

FROM: [redacted]

SUBJECT: HHS-OIG-OAS Draft Report: *A Large Northeastern Hospital Could Improve Certain Security Controls for Preventing and Detecting Cyberattacks* (A-18-22-08019)

Dear Ms. Lilly:

[redacted] (the "Hospital") appreciates the opportunity to respond to the U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services ("HHS-OIG-OAS") draft report, *A Large Northeastern Hospital Could Improve Certain Security Controls for Preventing and Detecting Cyberattacks* (A-18-22-08019). Given health care's growing reliance on information technology for patient care, telemedicine, and records, the Hospital recognizes the heightened importance of cybersecurity in this context. The Hospital appreciates HHS-OIG-OAS's role in guiding and supporting the adoption of cybersecurity measures to protect patients and health care delivery systems from cyberattacks. We take cybersecurity seriously and value your attention to this matter. Please find our comments and response to the draft report recommendations below.

HHS-OIG-OAS RECOMMENDATION 1

Enforce and periodically assess compliance with its configuration and change management policy, which requires that a security impact analysis be performed for all newly deployed or modified systems, including contractor-deployed systems, and that any discovered issues or unsecure configuration settings are resolved before a system is deployed or exposed to the internet.

HOSPITAL RESPONSE

The Hospital concurs with this recommendation. The Hospital has a process in place to enforce and periodically assess compliance with the its configuration and change management policy. The Hospital's security impact analysis process includes an architecture review to ensure that systems are secured and configured in accordance with approved security standards and baselines. Scans are conducted to identify and remediate vulnerabilities, with security approval required prior to deployment.

Additionally, the Hospital conducts periodic security reviews of contractor-deployed solutions prior to procurement and upon major system changes. The Hospital will continue to focus on contractor-deployed systems in its reviews and enforce remediation of any critical issues or misconfigured settings before a system is deployed or exposed to the internet.

HHS-OIG-OAS RECOMMENDATION 2

Periodically assess and update its identification and authentication controls in its systems to ensure: (1) users are uniquely identified and authenticated; (2) strong authentication and authenticators (e.g., passwords) have sufficient strength to prevent common cyberattacks against authentication controls (e.g., password spraying); and (3) feedback of authentication information during the authentication process is not disclosed.

HOSPITAL RESPONSE

The Hospital concurs with this recommendation and is committed to maintaining robust identification and authentication controls. The Hospital has a process in place to periodically assess and update its identification and authentication controls to align with NIST guidelines and best practices. The Hospital's current password policy and processes include measures to ensure (1) users are uniquely identified and authenticated; (2) strong authentication and authenticators have sufficient strength to prevent common cyberattacks against authentication controls; and (3) feedback of authentication information during the authentication process is not disclosed. For example, the Hospital requires multi-factor authentication ("MFA") for remote access, employee administrative systems, and access to certain key applications, such as email.

The Hospital is evaluating additional solutions to further enhance and strengthen its authentication and security controls. Initiatives underway include implementing an Identity and Threat Detection Response ("ITDR") solution to detect compromised or breached passwords and require password changes for affected users, as well as further expanding implementation of the MFA solution to cover additional use cases such as desktop access.

HHS-OIG-OAS RECOMMENDATION 3

Periodically assess and update its configuration management controls in its systems to ensure: (1) information system flaws are identified and timely corrected; (2) configuration settings for IT products on its systems are secure and in compliance with established configuration baselines; and (3) systems functionality, including functions, ports, protocols, and services are limited to only those that are necessary.

HOSPITAL RESPONSE

The Hospital concurs with this recommendation. The Hospital has processes in place to periodically assess and update its configuration management controls to ensure that misconfigurations are identified and addressed in a timely manner. The Hospital conducts ongoing vulnerability and configuration scans to identify exposures requiring remediation, using a risk-based approach. The Hospital will continue to work with the application teams and vendors as appropriate to enforce stricter controls, including compliance with remediation timelines and maintenance of configuration baselines.

HHS-OIG-OAS RECOMMENDATION 4

Establish a policy or process to periodically assess its internet-accessible systems and applications security controls against security control standards from NIST SP 800-53 or similar industry web application security standards and promptly resolve any identified weaknesses.

HOSPITAL RESPONSE

The Hospital concurs with this recommendation. The Hospital has established policies and processes to regularly review its internet-accessible systems by performing ongoing vulnerability scans. Internet facing and internal devices are scanned regularly, and independent penetration tests are conducted at least annually for externally facing assets and other critical internal systems.

The Hospital utilizes (1) a third-party vendor to continuously monitor publicly facing servers and (2) a cyber risk monitoring service to identify third-party partner risk. The Hospital will continue to review its policies, processes, and security controls to ensure they are properly updated to reflect industry best practices and NIST guidelines (e.g., security control standards from NIST SP 800-53) and will further enhance its controls as necessary.

HHS-OIG-OAS RECOMMENDATION 5

Implement a policy that requires developers to follow secure coding practices for its web applications in accordance with the Entity's approved cybersecurity framework or industry web application security best practices for coding, testing, and maintaining web applications and establish a procedure to confirm adherence to the requirements.

HOSPITAL RESPONSE

The Hospital concurs with this recommendation and has updated its policies to include requirements for secure coding practices for internally developed applications using "Security by Design" principles such as input validation, secure error handling, secure data storage, and protection against common security vulnerabilities. Additionally, the Hospital has established a Secure Software Development Governance Committee to oversee secure development for its web applications and adherence to secure coding practices. Further, as discussed above, the Hospital has procedures in place to ensure web application security best practices are implemented and maintained.

We appreciate the opportunity to review and comment on this draft. Please direct any follow-up inquiries to me at [redacted]

Sincerely,

[redacted]

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