GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Snapshot

# Healthcare Cybersecurity: HHS Continues to Have Challenges as Lead Agency

GAO-25-107755 · November 2024

As the lead federal agency for the healthcare and public health critical infrastructure sector, the Department of Health and Human Services (HHS) has faced challenges in carrying out its cybersecurity responsibilities. Implementing our related prior recommendations can help HHS in its leadership role.

## The Big Picture

Over the last several years, there have been increased cyberattacks in the healthcare and public health critical infrastructure sector. Recently, in February 2024, Change Healthcare (a health payment processor) became the victim of a ransomware cyberattack that involved the theft of data resulting in estimated losses of $874 million and widespread impacts on healthcare providers and patient care.

**Illustration of Example Ransomware Cyberattack Impacts**


Sources: GAO analysis of publicly reported incident information; GAO (sign); archipoch/stock.adobe.com (hospital); elenabsl/stock.adobe.com (images). | GAO-25-107755

As the lead federal agency for the healthcare and public health sector, HHS is responsible for strengthening cybersecurity in the sector. These responsibilities include coordinating with the Cybersecurity and Infrastructure Security Agency (CISA), the national coordinator for critical infrastructure security and resilience.

## What GAO's Work Shows

Our prior work has highlighted HHS' challenges in carrying out its lead responsibilities for sector cybersecurity. The department has not yet implemented all our recommendations to address these challenges.

### Supporting Healthcare Cyber Risk Management

HHS has several initiatives intended to mitigate ransomware risks for healthcare and public health. Nevertheless, our prior work has found that the department had not adequately monitored the sector's implementation of ransomware mitigation practices. For example, in January 2024, we reported that HHS released results of an analysis of U.S. hospitals' cybersecurity. Among other things, the analysis found that participating hospitals had self-assessed that they had adopted 70.7 percent of the National Institute of Standards and Technology Cybersecurity Framework's functional areas of identify, detect, protect, respond, and recover.

However, at the time of our report, HHS was not yet tracking adoption of the ransomware-specific practices outlined in the framework. Although HHS officials told us that they would be able to assess implementation of key concepts in the framework, the department did not provide evidence of its efforts to do so. Without full awareness of the sector's adoption of cybersecurity practices, HHS risks not directing resources where needed.

- We recommended that HHS, in coordination with CISA and sector entities, determine the sector's adoption of leading cybersecurity practices that help reduce ransomware risk.

Our January 2024 report also found that HHS had not evaluated the effectiveness of the support it provides to the sector. Specifically, we reported that HHS provided various types of support, such as guidance documents, training, job aids, and threat briefings to help the sector manage ransomware risks. However, the department did not demonstrate that it evaluated which type of support would be the most effective. As a result, the department could not fully address concerns about communication, coordination, and timely sharing of threat and incident information.

- We recommended that HHS, in coordination with CISA and sector entities, develop evaluation procedures to measure the effectiveness of its support in helping to reduce ransomware risk.

**Assessing Sector Cybersecurity Risks**

In addition to IT, the sector relies on Internet of Things (IoT) and operational technology (OT) devices and systems to provide essential healthcare and public health services. In December 2022, we reported that HHS had ongoing risk activities for medical devices, a specific type of IoT device. However, HHS had not conducted a comprehensive sector-wide cybersecurity risk assessment addressing IoT and OT devices. As a result, the department did not know what additional security protections were needed to address growing and evolving threats.

- We recommended that HHS include IoT and OT devices as part of the risk assessments of the sector's cyber environment.

**Coordinating and Collaborating for Sector Cybersecurity**

Within HHS, the Administration for Strategic Preparedness and Response (ASPR) is responsible for leading collaboration efforts to strengthen the security and resilience of the sector. In June 2021, we reported that ASPR was leading or co-leading several working groups focused on supporting the sector. In doing so, we determined that ASPR demonstrated most leading collaboration practices for those working groups. However, it did not fully or consistently:

- monitor the working groups' progress towards meeting defined goals,
- clarify responsibilities for carrying out the groups' roles, or
- regularly update the charter describing how the working groups are to collaborate.

As a result, ASPR could not ensure that it was effectively collaborating to improve cybersecurity.

- We recommended that ASPR take action to fully and consistently demonstrate leading collaboration practices.

Our May 2020 report found that the Centers for Medicare and Medicaid Services (CMS)—an HHS component agency—established cybersecurity requirements to protect the data that it shares with state government agencies. However, these requirements often had parameters that conflicted with those established by other federal agencies that share data with states, such as the Social Security Administration. An example of a conflicting parameter is agencies defining different values for the number of consecutive unsuccessful log-on attempts prior to user lockout. We also determined that while CMS had policies in place for coordinating with state agencies when assessing states' cybersecurity, they did not have such policies on coordinating with other federal agencies on the assessments.

The conflicting parameters can place an unnecessary burden on state officials' time and resources. This in turn could lead to reduced attention on other important cybersecurity efforts.

- We recommended that CMS solicit input from relevant federal agencies on revisions to its security policy to ensure consistency across cybersecurity requirements for state agencies. We also recommended that CMS revise its assessment policies to maximize coordination with other federal agencies.

Until HHS implements our prior recommendations related to improving cybersecurity, the department risks not being able to effectively carry out its lead agency responsibilities, resulting in potential adverse impact on healthcare providers and patient care.



**Contact Us:**

For more information, contact: Jennifer R. Franks, FranksJ@gao.gov, (404) 679-1831.

Sarah Kaczmarek, Managing Director, Public Affairs, KaczmarekS@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Contributors: Chris Businsky, Brandon Cox, Jonnie Genova, Darron Smallwood, Di'Mond Spencer (Assistant Director), and Ibrahim Suleman (Analyst-in-Charge).

Source (cover photo): BillionPhotos.com/stock.adobe.com.