GAO Highlights

Highlights of GAO-24-106683, a report to congressional committees

December 2023

# MEDICAL DEVICE CYBERSECURITY

## Agencies Need to Update Agreement to Ensure Effective Coordination

## Why GAO Did This Study

Cyber threats that target medical devices could delay critical patient care, reveal sensitive patient data, shut down health care operations, and necessitate costly recovery efforts. FDA is responsible for ensuring that medical devices sold in the U.S. provide reasonable assurance of safety and effectiveness.

The Consolidated Appropriations Act, 2023, includes a provision for GAO to review cybersecurity in medical devices. This report addresses the extent to which (1) relevant non-federal entities are facing challenges in accessing federal support on medical device cybersecurity, (2) federal agencies have addressed identified challenges, (3) key agencies are coordinating on medical device cybersecurity, and (4) limitations exist in agencies' authority over medical device cybersecurity.

GAO identified federal agencies with roles in medical device cybersecurity. It also selected 25 non-federal entities representing health care providers, patients, and medical device manufacturers. GAO interviewed these entities on challenges in accessing federal cybersecurity support. In addition, GAO assessed agency documentation and compared coordination efforts against leading collaboration practices; reviewed relevant legislation and guidance; and interviewed agency officials.

## What GAO Recommends

GAO is making recommendations to FDA and CISA to update their agreement to reflect organizational and procedural changes that have occurred. Both agencies concurred with the recommendations.

View GAO-24-106683. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

## What GAO Found

According to the Department of Health and Human Services (HHS), available data on cybersecurity incidents in hospitals do not show that medical device vulnerabilities have been common exploits. Nevertheless, HHS maintains that such devices are a source of cybersecurity concern warranting significant attention and can introduce threats to hospital cybersecurity (see figure).

**Figure: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network**


1. Threat actor gains access to a healthcare provider's network by exploiting a vulnerability (e.g. a phishing attack).
2. Threat actor takes command of a server to which a patient heart monitor is attached.
3. While scanning the network, the threat actor takes control of all heart monitors and is able to shut them off, which puts additional patients at risk.
4. Threat actor could compromise other devices on the network, adding to patient risk.

Sources: GAO interpretation of Department of Health and Human Services example (illustrations); gofficon/stock.adobe.com (icons); elenabsl/stock.adobe.com (illustrations). | GAO-24-106683

Non-federal entities representing health care providers, patients, and other relevant parties identified challenges in accessing federal support to address cybersecurity vulnerabilities. Entities described challenges with (1) a lack of awareness of resources or contacts and (2) difficulties understanding vulnerability communications from the federal government. Agencies are taking steps that, if implemented effectively, can meet these challenges.

Key agencies are also managing medical device cybersecurity through active coordination. Specifically, the Food and Drug Administration (FDA) and the Cybersecurity and Infrastructure Security Agency (CISA) developed an agreement addressing most leading practices for collaboration. However, this 5-year-old agreement did not address all such practices and needs to be updated to reflect organizational and procedural changes that have occurred since 2018.

FDA authority over medical device cybersecurity has recently increased. Specifically, December 2022 legislation requires medical device manufacturers to submit to FDA, among other things, their plans to monitor, identify, and address cybersecurity vulnerabilities for any new medical device that is to be introduced to consumers starting in March 2023. This legislation is limited to new devices and does not retroactively apply to those devices introduced prior to March 2023, unless the manufacturer is submitting a new marketing application for changes to the device.

FDA officials are implementing new cybersecurity authorities and have not yet identified the need for any additional authority. They can take measures to help ensure device cybersecurity under existing authorities such as monitoring health sector and CISA alerts, as well as directing manufacturers to communicate vulnerabilities to user communities and to remediate the vulnerabilities.

According to FDA guidance, if manufacturers do not remediate vulnerabilities, FDA may find the device to be in violation of federal law and subject to enforcement actions.