Health-ISAC Press Materials

What is Health-ISAC?

Health-ISAC (Health Information Sharing and Analysis Center) serves critical infrastructure owners and operators within the Health and Public Health sector (HPH). Health-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating, and sharing vital physical and cyber threat intelligence and best practices. The community is focused on sharing timely, actionable, and relevant information, including intelligence on threats, incidents, and vulnerabilities, especially regarding coordinated disclosure efforts. Health-ISAC also fosters relationships and networking through educational events and discussions. Working groups and committees connect on important topics and produce white papers for public sharing.

HEALTH-ISAC regularly engages with external partners such as government, law enforcement, the vendor community, other ISACs, and HPH associations, such as the Healthcare and Information Management Systems Society (HIMSS), the Electronic Healthcare Network Accreditation Commission (EHNAC), and the College of Healthcare Information Executives (CHIME), to facilitate situational awareness and inform risk-based decisions.

What's Included in This Kit?

This kit provides background information on medical device security.

How Do I Use It?

Review this kit to learn more about the current security landscape and how industry partners address potential security vulnerabilities in medical devices.

Contents

FDA FAQ

The Food and Drug Administration (FDA) has developed a Cybersecurity in Medical Devices Frequently Asked Questions (FAQs) to help explain regulations impacting medical device cybersecurity.

Medical Device Security/Cybersecurity Media Backgrounder

The following is an overview of medical device/cybersecurity and how industry partners work together. **The landscape has evolved, and many industries are impacted**.

- Security vulnerabilities are not unique to the medical device industry. Everyone with a smartphone installs periodic software updates when they are released (typically several times a year). Some automotive companies update their products over the air, without requiring drivers to visit a service location for a fix. Even television sets download and update software from time to time. Medical devices also need to be updated as technology evolves. The medical device industry is no different than other Internet of Things ("IOT") devices.
- Disclosures, and increased transparency, are a sign of increased company responsibility and accountability– not an admission of fault. Many organizations operating in high-tech fields are issuing security vulnerability notices.
- Most companies follow coordinated disclosure processes (see separate coordinated vulnerability disclosure document - LINK) that encourage transparency in the communication of vulnerable products to the clinician and patient community. These processes, which may be documented on a company's external website, guide the steps taken when a security concern is identified and help ensure that the matter is communicated and addressed transparently.

Cybersecurity Guidance Is Relatively New – and Still Evolving

- On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus—"Ensuring Cybersecurity of Medical Devices"—amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The information provided on this page may be useful for sponsors in preparing their premarket submissions. The FDA has released pre- and post-market cybersecurity guidance for manufacturers to consider in the design, development, deployment, and maintenance of medical devices. Although this is focused on the US market, many other regulatory agencies outside the US are leveraging the themes and concepts introduced by the FDA in these guidance documents.
    - **Premarket guidance** cybersecurity design, development, testing, monitoring, and response recommendations (finalized by the FDA in September 2023) for medical device makers seeking approval to market their devices in the United States.
    - **Postmarket guidance** recommendations (finalized by the FDA in December 2016) outline comprehensive management of cybersecurity vulnerabilities for marketed and distributed medical devices throughout the product lifecycle.
    - **Select Updates** (draft guidance released for comment in March 2024) identifies the cybersecurity information the FDA considers to generally be necessary to support obligations under section 524B of the FD&C Act.
- Medical device manufacturers and healthcare delivery organizations work closely with regulatory bodies to review and understand these guidance documents to most effectively incorporate them into their organizations.

Consideration of Full Product Lifecycle

- Medical device manufacturers are working to manage supported devices in hospitals, clinics, or patient homes that are critical to delivering therapy. As the landscape evolves, those products need updating. Newer products have improved security controls because they are developed when expectations regarding security and the ability to update are different.
- Today, manufacturers develop products knowing they will be updated through their full lifecycle. This is typically accomplished by patching the device over its useful life.

Partnership and Collaboration

- Medical device manufacturers maintain close partnerships with various parties – including industry peers, security researchers, healthcare delivery organizations, customers, patients, and government agencies – to drive security, transparency, and information and intelligence sharing.

Device Manufacturer Coordinated Vulnerability Disclosure links

- Click here for access to medical device manufacturers' product security websites

Media Contact

- Health-ISAC: contact@h-isac.org