H-ISAC Press Materials

What is H-ISAC?

H-ISAC (Health Information Sharing and Analysis Center) is a group made up of critical infrastructure owners and operators within the Health and Public Health sector (HPH). H-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 relating to coordinated disclosure efforts. H-ISAC also fosters relationship building and networking through educational events and discussions. Working groups and committees connect on important topics and produce white papers for public sharing.

H-ISAC is regularly engaged 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 decision making.

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 Glossary of Terms

The Center for Devices and Radiological Health (CDRH) within the Food and Drug Administration (FDA) group has developed a glossary to help explain cybersecurity terms.

Medical Device Security/Cybersecurity Media Backgrounder

The following is an overview on the state 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 smart phone 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 make a trip 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 helps ensure that the matter is communicated and addressed in a transparent way.

Cybersecurity Guidance Is Relatively New – and Still Evolving

- In the past five years, the FDA has released pre- and postmarket cybersecurity guidance, designed to help manufacturers consider cybersecurity 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** recommendations (finalized by FDA in October 2014) help facilitate an efficient review process as a device maker is seeking approval to sell the device and ensures they are designed to sufficiently address cybersecurity threats before the devices are on the market.
    - **Postmarket guidance** recommendations (finalized by FDA in December 2016) outline comprehensive management of cybersecurity vulnerabilities for marketed and distributed medical devices throughout the product lifecycle.
- 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 often working to manage fielded, supported devices (those that are currently in use in hospitals, clinics, or patient homes and still supported by the manufacturer) that are critical to delivering therapy. As the landscape evolves, those products need updating. Newer products have more rigid security standards because they are developed in a time when expectations specifically regarding security and the ability to update are different.
- Today, manufacturers develop products knowing they will need to be updated through its 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.

Media Contact

- H-ISAC: contact@h-isac.org
- Click here for access to medical device manufacturers' product security websites