H-ISAC Press Materials

What is H-ISAC?

H-ISAC (Health Information Sharing and Analysis Center) 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.

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
- Medical Device Security/Cybersecurity Media Backgrounder
- Coordinated Vulnerability Disclosure Process (LINK)
- Media Contacts

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 Landscape Has Evolved, and Many Industries Are Impacted

- Security vulnerabilities are not unique to the medical device industry. Vulnerabilities occur across a range of industries, from the financial sector to transportation to infrastructure to consumer goods. For example, everyone with a smart phone installs periodic software updates when they are released (typically several times a year).
- Disclosures, and increased transparency, are a sign of increased company responsibility and accountability – not an admission of fault.
- Most companies follow coordinated disclosure processes that encourage transparency in the communication of vulnerable products to the clinician and patient community.

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 and development of medical devices.

  - **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.

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, updates need to be made to those products.
- Today, manufacturers develop products knowing they will need to be updated through its full lifecycle.

Partnership and Collaboration

- Medical device manufacturers maintain close partnerships with 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