HAVE YOU HEARD ABOUT PROTECTING MEDICAL DEVICES?

Medical device security is an essential element for protecting patient safety. These devices deliver significant benefits and are the cornerstone for patient care. As with all technologies, medical devices are accompanied by cybersecurity challenges. Due to greater connectivity and features, certain devices may now be vulnerable to cyber threats. In this issue of Have You Heard, we will provide resources that can assist your organization in making medical devices cyber safe.

BY THE NUMBERS

16%
INCREASE IN IoT VULNERABILITIES

0.4%
INCREASE IN VULNERABILITIES OVERALL

The number of vulnerabilities related to **Internet of Things devices increased by 16%** year over year, compared to a growth rate of only **0.4% for vulnerabilities** overall.

SOURCE: https://www.ibm.com/security/data-breach/threat-intelligence/

Year over year, the number of breaches reported **increased 19%:** there were **905** reported in 2021, compared to **758 in 2020.**

758 IN 2020
905 IN 2021

SOURCE: https://www.protenus.com/breach-barometer-report

48 percent of data lost was on a **laptop, desktop computer, or mobile device.**

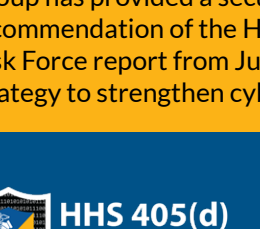
SOURCE: https://www.kiteworks.com/hipaa-compliance/lost-stolen-mobile-devices-leading-cause-of-healthcare-data-breaches/

LOOKING FOR MORE INFORMATION?

Check out the resources below!

HHS 405(d)—Aligning Health Care Industry Security Approaches

405(d) aims to enhance cybersecurity and align health industry security approaches by developing best practices and mitigation strategies to attack the most common cyber threats facing the health sector. Healthcare organizations should check out The *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP) Main Document, Practice #9 on Connected Medical Device Security to ensure their medical devices are cyber secure.


Staying Resilient to Medical Device Attacks

Medical Device Attacks Mitigation Practices to Consider

How Can You Mitigate Medical Device Attacks?

RESOURCES

- June Spotlight Webinar—The Internet of Medical Things: Making Them More Secure
- Prescription Poster—Medical Devices
- Five Threat Series Flyer—Attacks on Medical Devices
- Threat Series Slides—Attacks on Connected Medical Devices
- Poster—Put Patients First: Protect Connected Medical Devices
- HICP

The Food and Drug Administration (FDA)

The Food and Drug Administration (FDA), an agency within the U.S. Department of Health and Human Services, has four directorates overseeing the core functions of the agency:

1. Medical Products and Tobacco,
2. Foods and Veterinary Medicine,
3. Global Regulatory Operations and Policy, and
4. Operations.

A core responsibility is protecting the public health by assuring the safety, effectiveness, quality, and security of human and veterinary drugs, vaccines and other biological products, and medical devices. The FDA has released multiple resources and guidance on securing your medical devices and protect against loss of protected health information.

RESOURCES

- Digital Health Center of Excellence—Cybersecurity Homepage
- Digital Health Center of Excellence—Medical Device Interoperability
- Digital Health Center of Excellence—Software as a Medical Device

Health Sector Cybsersecurity Coodination Center (HC3)

HC3 provides recommendations and mitigation strategies around medical device security, for protecting the sector against cyber threats especially threats that impact patient safety, security, and privacy. In addition, they have created guidance on threat modeling for mobile health systems that will help you to understand your systems complexity. Therefore, helping you to understand all possible threats that could affect your medical devices. For more information, please email HC3@hhs.gov.

RESOURCES

- SMB Vulnerabilities in Healthcare
- Threat Modeling for Mobile Health Systems
- HC3 Intelligence Briefing Wearable Device Security
- Medical Device Image Tampering

Department of Homeland Security (DHS)—Cybersecurity & Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure security agency CISA provides Cyber essentials toolkits with actionable practices that are consistent with NIST cybersecurity framework. Including additional resources that if implemented will support a proactive risk management culture and limit the risk of compromise of your medical devices.

RESOURCES

- Medical Device Management
- CISA Cyber Essentials Toolkit Chapter 3: Your Systems
- Cyber Hygiene Services

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) NIST was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake resistant skyscrapers and global communication networks. The practices found in HICP, like medical device security, are largely based on NIST frameworks.

RESOURCES

- Blog – "Securing Internet-Connected Medical Devices"

Healthcare and Public Health Sector Coordinating Council (HSCC)

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan. They partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group has provided a security plan to address a major recommendation of the Health Care Industry Cybersecurity Task Force report from June 2017 calling for a cross-sector strategy to strengthen cybersecurity in medical devices.

RESOURCES

- Health Industry Cybersecurity Supply Chain Risk Management Guide V2.0 (HIC-SCRiM-V2)
- Medical Device and Health IT Joint Security Plan (JSP)

HHS 405(d)
Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov or our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*