# Health-ISAC Press Materials

## Coordinated Vulnerability Disclosure Process

The following information highlights the coordinated vulnerability disclosure (CVD) process utilized by companies.

### Background

- FDA guidance documents state that medical device cybersecurity concerns must be addressed not only during the design and development of medical devices, but also throughout the product lifecycle, as potential vulnerabilities emerge.
- Medical device manufacturers (MDMs) use a variety of policies, processes, and procedures to manage cybersecurity risk. One proven way to manage some cybersecurity risks is the implementation of CVD policies and processes. This is evidence of a maturing medical device industry continuing to enhance its communication, collaboration, transparency, and risk mitigation capabilities in the evolving cybersecurity space.
- As the disclosure of cybersecurity vulnerabilities in the medical device industry becomes more common, perceptions about vulnerability disclosure should become more positive, as the disclosures are an effort toward responsible continuous quality improvement and risk management.

### Process Overview

- **Reporting:** Many MDMs welcome vulnerability reports from security researchers, customers, third-party vendors, and other groups or individuals who wish to report a vulnerability in a software-enabled device.
- **Analysis:** MDMs often collaborate with the reporter of the vulnerability to analyze, confirm, and disclose the vulnerability.
- **Coordination:** If the vulnerability is confirmed, MDMs may perform a cybersecurity risk assessment and clinical risk assessment to further evaluate the vulnerability. If applicable, the MDM will conduct validation and remediation planning while notifying and reporting to various stakeholders. These stakeholders typically include the FDA and the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS), who are important collaboration partners.
- **Disclosure:** Through the CVD process, the MDM normally publishes the contents of the notification on their website and voluntarily reports to ISACs, ISAOs and other partners to share and notify customers of any potential risks in a transparent format. Some vulnerabilities are also publicized via a DHS CISA Advisory to enhance transparency and awareness.
- This CVD process that many MDMs have adopted continues to proactively address product security in an everchanging environment to reduce risks posed to patients.

### Media Contact

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