FDA Cybersecurity Regulation

Brian Holdsworth

Focus 42 LLC

FDA Role

The FDA has published premarket and postmarket guidances that offer recommendations for the comprehensive management of medical device cybersecurity risks. Additionally, the reduction of security risks through continuous improvement over the course of the device's life-cycle is mandated.

> The FDA encourages medical device manufacturers to address cybersecurity risks to keep patients safe and better protect the public health. This includes monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market.
>
> — U.S. FDA

Through the FDA's longstanding regulations regarding Quality Systems (QSR), device manufacturers are **required to address all risks, including cybersecurity risk**. The FDA's Cybersecurity guidances provide their recommendations for manufacturers to meet the QSR.

Risks

Device Risks

Modern medical devices frequently make use of embedded microprocessor technology, computer networking technology (wired and wireless), and externally networked computing infrastructure. Such advanced IT solutions can improve both patient care and health care efficiency. However, like all other IT and computing solutions, these systems are vulnerable to security breaches. Depending on the classification of the device, a security breach that impacts its functionality could pose risk of serious injury or death to the patient.

Patient Privacy Risks

Data breaches of systems that contain electronic patient health information (ePHI) are another category of security risk that arise during the development of modern medical devices. Patients' privacy is protected by U.S. Federal Regulations known as the *Health Insurance Portability and Accountability Act (HIPAA)*. As such, the manufacturers and users of networked medical devices are potentially liable for data breaches that threaten the patients' privacy.

All risks related to cybersecurity vulnerabilities must be identified, and mitigations established, as part of the medical device's design-control procedure. Thus, all software associated with the device should be designed to meet specific security requirements by software engineers who have been properly trained on the requirements. Verification & validation activities must also specifically address these documented security requirements.

Costs of Non-compliance

Medical device manufacturers that fail to adhere to QSR Regulations by designing devices that do not adequately address cybersecurity vulnerabilities may be subject to FDA enforcement actions (e.g. seizure, injunction, civil money penalties, and criminal prosecution). Additionally, data breaches are very costly to remediate, and vendors of medical devices deemed to have security

design flaws risk being liable for such costs.

> The biggest financial consequence to organizations that experienced a data breach is lost business.
>
> — IBM, 2016 Security Intelligence survey

IBM's survey concluded that the average cost in lost business of a data breach was $4,000,000 USD. Additionally, the average cost of a health care information breach was **$355 PER Patient Record**. The costs of a data breach to businesses has also been increasing at a rate of ~10% per year.

A Comprehensive Solution

The best way to identify and mitigate the security risks of a modern medical device is to engage directly with the IT Security Industry, which has well-established best practices for addressing these risks at every stage of the product life-cycle.

Focus 42 LLC has developed a program tailored to the needs of medical device manufacturers and based on IT Security Industry best practices. We are closely aligned with practices defined by the *Center for Internet Security (CIS)*, and can assist your company in using certified security professionals to develop the multi-faceted procedures needed to manage your security risks.

CIS Critical Security Controls