DigiCert® Device Trust

# DIGITAL TRUST IN CONNECTED HEALTHCARE

Building IoMT Excellence with DigiCert Device Trust

## Overview

The landscape of healthcare is evolving, with innovations such as the Internet of Medical Things (IoMT) reshaping how medical devices operate, communicate, and deliver vital patient data. These innovations are driving new security requirements for protecting attack surfaces, data, and communication. Organizations can consider the following questions as inputs to developing effective device security strategies that address patient safety, regulatory compliance, and scalability needs.

## Assessment

**Uncovering Vulnerabilities:** Do you know the types of vulnerabilities that may lurk in your IoT devices? Safeguarding IoMT hinges on discovering these vulnerabilities before deploying code to your devices.

**Fostering Vigilance:** Does your current security approach anticipate threats? The difference between resilience and vulnerability lies in proactive security measures.

**Balancing Priorities:** Do current security practices and innovation align? Striking the balance between advancement and security ensures trust and reputation.

**Partnering for Security:** Do your partners prioritize security to ensure your ecosystem is safe? Secure collaborations require partner commitment to safeguarding devices.

**Risk Tolerance:** What level of risk is your organization willing to accept, particularly for patient well-being and data integrity?

## Defining Requirements

**Assessing Security Needs:** Begin by evaluating the unique security requirements of your medical devices. Consider the type of data they handle, their connectivity, and potential vulnerabilities.

**Understanding Compliance:** Familiarize yourself with the regulatory standards that govern medical device security, such as HIPAA, FDA guidelines, and other relevant industry regulations.

## Vendor Selection

**Evaluating Vendor Expertise:** Look for vendors with a proven track record in medical device security. Investigate their experience, industry partnerships, and reputation.

**Scalability and Flexibility:** Ensure that your chosen solution can scale as your division expands. It should accommodate both existing and future devices seamlessly.

DigiCert® Device Trust

# DIGITAL TRUST IN CONNECTED HEALTHCARE

Building IoMT Excellence with DigiCert Device Trust

## Implementing Device Security

**Collaboration and Training:** Consider how Device Trust will be integrated into your product. Ensure that your chosen solution comes with comprehensive training and support for seamless implementation.

**Ongoing Maintenance and Updates:** Evaluate your solution's maintenance requirements and the ease of managing device security updates over time.

## Socializing with Stakeholders

**Consulting Stakeholders:** Involve key stakeholders within your division, including R&D, product, and security teams, to ensure a well-rounded assessment of your security needs.

**Cost-Benefit Analysis:** Conduct a thorough cost-benefit analysis to determine the financial implications of implementing the chosen solution.

## Making an Informed Decision

Incorporating Device Trust into your security strategy is more than a choice; it's a calculated step towards safeguarding the future of your medical devices. By establishing a defense against potential threats, Device Trust delivers data protection, ensures regulatory compliance, and fosters patient trust.

To explore how Device Trust can fortify your organization's medical devices and security landscape, reach out to us at sales@digicert.com.