THE 7 HABITS OF HIGHLY TRUSTWORTHY MEDICAL DEVICES

digicert®

1 ESTABLISHES AN ORGANIZATION–SPECIFIC ROOT OF TRUST (ROT)

Cryptographic encryption and certificates of authentication establish and preserve device trustworthiness throughout the lifecycle, ensuring the integrity of data harvested and processed by artificial intelligence (AI) and machine learning (ML) engines.

2 REDUCES LIFETIME COSTS TO MANUFACTURERS, PROVIDERS AND PATIENTS

Manufacturing, deployment and lifetime monitoring of connected and edge devices are automated and scalable, decreasing operational expenses for OEMs and healthcare organizations and reducing the cost of life-saving patient care.

3 MANAGES SUPPLY–CHAIN RISKS

Automated code-signing workflows reduce the attack surface in the software development lifecycle (SDLC), providing tamper-resistant content delivery that's tracked and traced from the developer all the way through to the target OT device.

4 RECOVERS TO A TRUSTED STATE

Field device recovery, image and configuration rollbacks, and cryptographic artifact rotation are performed remotely, mitigating service outages and minimizing exposure to potential exploits.

5 PROTECTS AT-REST, IN-PROCESS AND IN-TRANSIT DATA

A secure element acts as the hardware-, firmware- or software-based root of trust, protecting data in the custody of mission-critical native and/or containerized applications.

6 ACHIEVES AND MAINTAINS COMPLIANCE

Software is encryption-enabled and regularly updated to comply with GDPR, HIPAA and other regulations. Role-based user access controls prevent unauthorized users from accessing the device or its accompanying data.

7 FOLLOWS A ZERO-TRUST SECURITY MODEL

The device is part of a Zero-Trust framework that uses PKI to authenticate the identity of all users and devices on the network, encrypting every communication and maintaining the data coming to and from users and devices.

In the fight for device safety, manufacturers are on the frontlines. But we're here to help. Reach out to sales@digicert.com to take the first step toward securing your medical devices.