Biomed & Internet of Things (IoT) Cybersecurity Readiness

ecfirst

Biomed Facts: FBI

- The number of internet-connected medical devices is projected to grow from 20 billion in 2018 to 50 billion in 2020.
- Deficient security capabilities, legacy operating systems, difficulties in patching vulnerabilities and a lack of security awareness are significant risks to both medical devices themselves and the networks to which they connect.
- Unsecure or poorly secured medical devices can leave networks open to Distributed Denial of Service (DDoS) attacks.

Source: FBI Alert I-101717a-PSA

Myth	Fact
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with other federal government agencies, such as the U.S. Department of Homeland Security (DHS), but also works with members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of critical cyber infrastructure.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review medical device updates implemented solely to strengthen cybersecurity.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

Securing IoT & Biomed Devices

- Equipment Management
- Patch Management
- Staff Security Training
- Vulnerability Scanning
- Risk Management
- RFP Language to Include Security Features
- Device Integration Test Lab

Biomed Devices

- Pacemakers
- Drug Pumps
- Mobile Medical Systems
- In-Home Monitors
- Personal Fitness Devices
- Medical Ventilators
- Medical Monitors
- Medical Imaging Machines

ecfirst Biomed & IoT Cybersecurity Services

- Biomed Risk Assessment (HIPAA, HITRUST®, NIST Cybersecurity Framework)
- Biomed Cybersecurity Assessment
- Biomed Policy and Procedure
- Biomed Cybersecurity Remediation
- Complimentary seat in industry leading Certified Cyber Security Architect℠ (CCSA℠) program
- Knowledge transfer throughout the biomed cybersecurity assessment
- Unconditional Guarantee. No Questions! ecfirst will not consider an engagement complete unless client is 100% satisfied

Biomed Business Risks

- Disruption of patient care
- Loss of Protected Health Information (PHI) and Personally Identifiable Information (PII)

Biomed & IoT Cybersecurity Readiness

The ecfirst Biomed and IoT Cybersecurity Report includes an Asset Inventory, which identifies specific biomed device information such as:

- IP Address
- Hostname (if resolvable or successfully authenticated)
- Operating System (if discoverable or successfully authenticated)
- Open Ports
  - Potentially Active Services
- Installed Software

Training & Certification

CCSA℠
Certified Cyber Security Architect

- Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework.
- Step through key areas that must be addressed in a credible incident response plan.
- Walk through core components, organization and CMMC Maturity Levels. Examine CMMC domains and CMMC capabilities required for organizations.

ecfirst Biomed Cybersecurity Checklist

- **Cybersecurity Framework** Determine the cybersecurity framework that will establish the foundation for your security program requirements for medical IoT devices.
- **Policy** Develop a cybersecurity policy specific to medical IoT devices. Ensure the policy is reviewed by associated and impacted departments/business units, approved by senior leadership, and communicated to the workforce.
- **Security Risk Assessment** Ensure medical IoT devices are within the scope of enterprise cybersecurity risk assessment exercises. Perform a vulnerability assessment to determine medical IoT device security gaps. Examine the security architecture and identify opportunities to possibly segregate medical IoT devices (i.e. determine application of segregation for medical IoT devices).
- **Business Associate Agreements (BAA)** Review third-party vendors (business associates) and their security practices to ensure HIPAA, FDA, and other mandates are appropriately addressed.
- **Configuration Management** Ensure each type of medical IoT device is configured consistently, and addresses the appropriate security capabilities to secure PHI and PII.
- **Encryption** Examine options to encrypt PHI and PII stored, processed or transmitted by medical IoT devices.
- **Risk Management** Based on the findings of the risk assessment, establish a plan for risk management of medical IoT devices. Ensure formal remediation is performed on a regular schedule (e.g. monthly).

Peter Harvey | PeterHarvey@ecfirst.com | www.ecfirst.com

ecfirst | AI Defense, Beyond Cyber