JOHNS HOPKINS UNIVERSITY

harborlabs™
CYBER . SCIENCE

Medical Device Security

A Thing Smart People Do

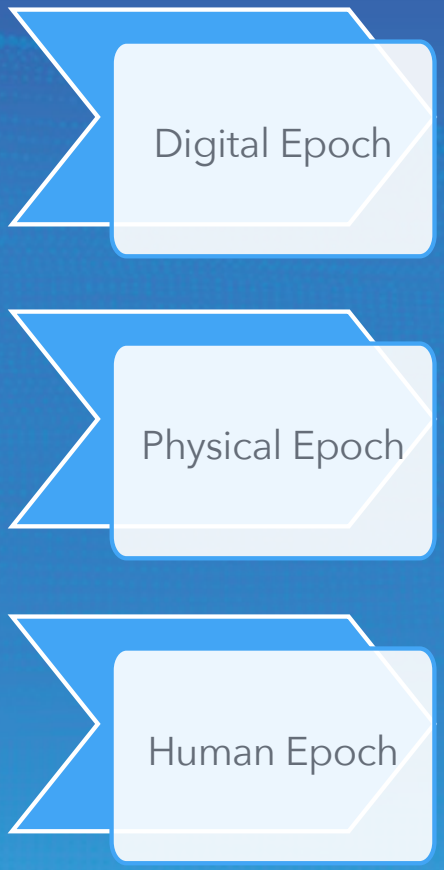
Dr. Avi Rubin

Director, Health and Medical Security Lab

Johns Hopkins University

Chief Scientist, Harbor Labs

Cyberattack Epochs



- The earliest form of hacking, the attack, the results, and the damages all occurred entirely in the digital word
- A relatively recent era, characterized by the use of digital tools to inflict damage in the physical world
- The use of the combined tools of the digital and physical worlds to inflict bodily damage in the human world

Water Treatment Plant attack

"All the News That's Fit to Print"

The New York Times

Late Edition

Today, morning clouds giving way to sunshine by the afternoon, high 65. Tonight, cloudy, low 54. Tomorrow, clouds giving way to sunshine, high 70. Weather map is on Page 23.

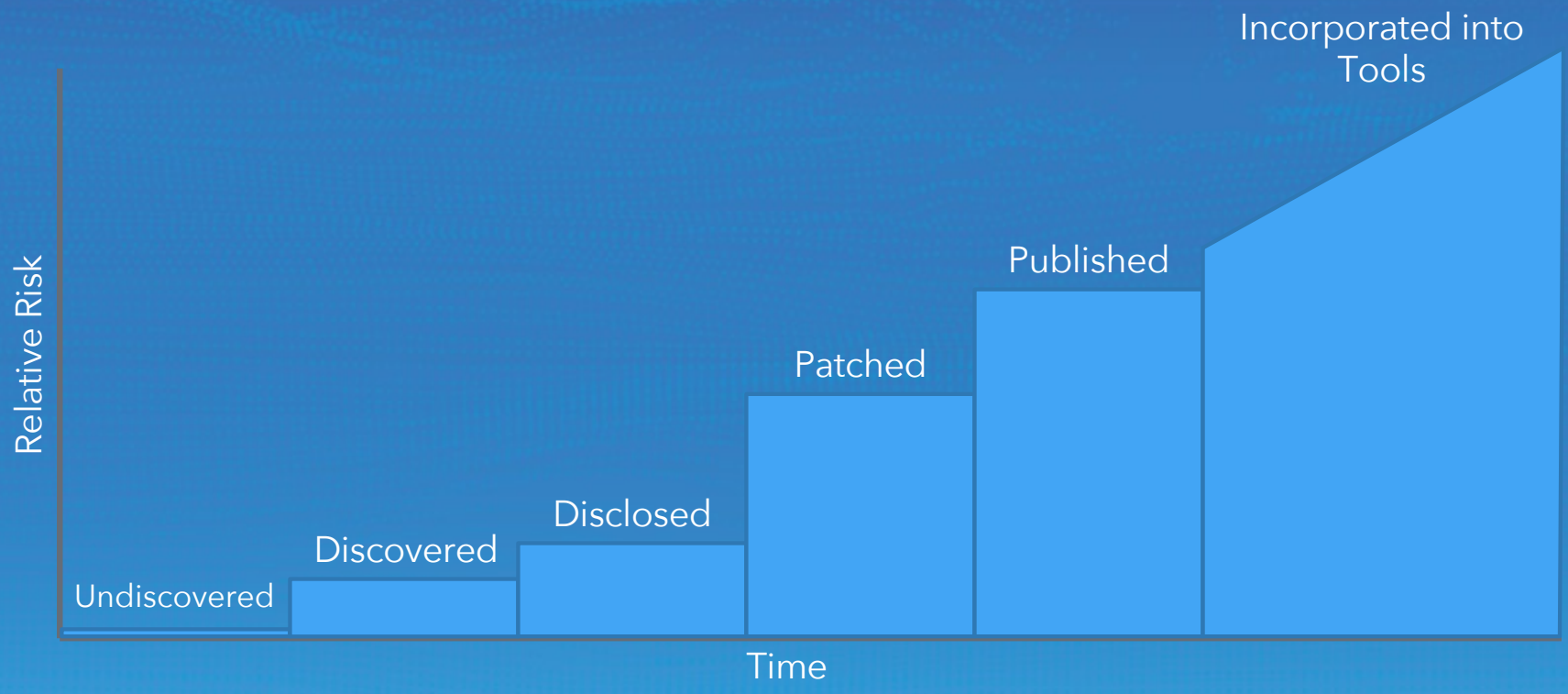
The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

- Feb 5, 2021 two days before Superbowl
- Sodium Hydroxide (drain cleaner)
  - Changed from 100 ppm to 11,100 ppm
- Remote Access credentials shared between employees
- TeamViewer software configured incorrectly
- Bigger issue: Why did the system plant even allow such a value?
- Was caught by a vigilant employee
- People could have died!

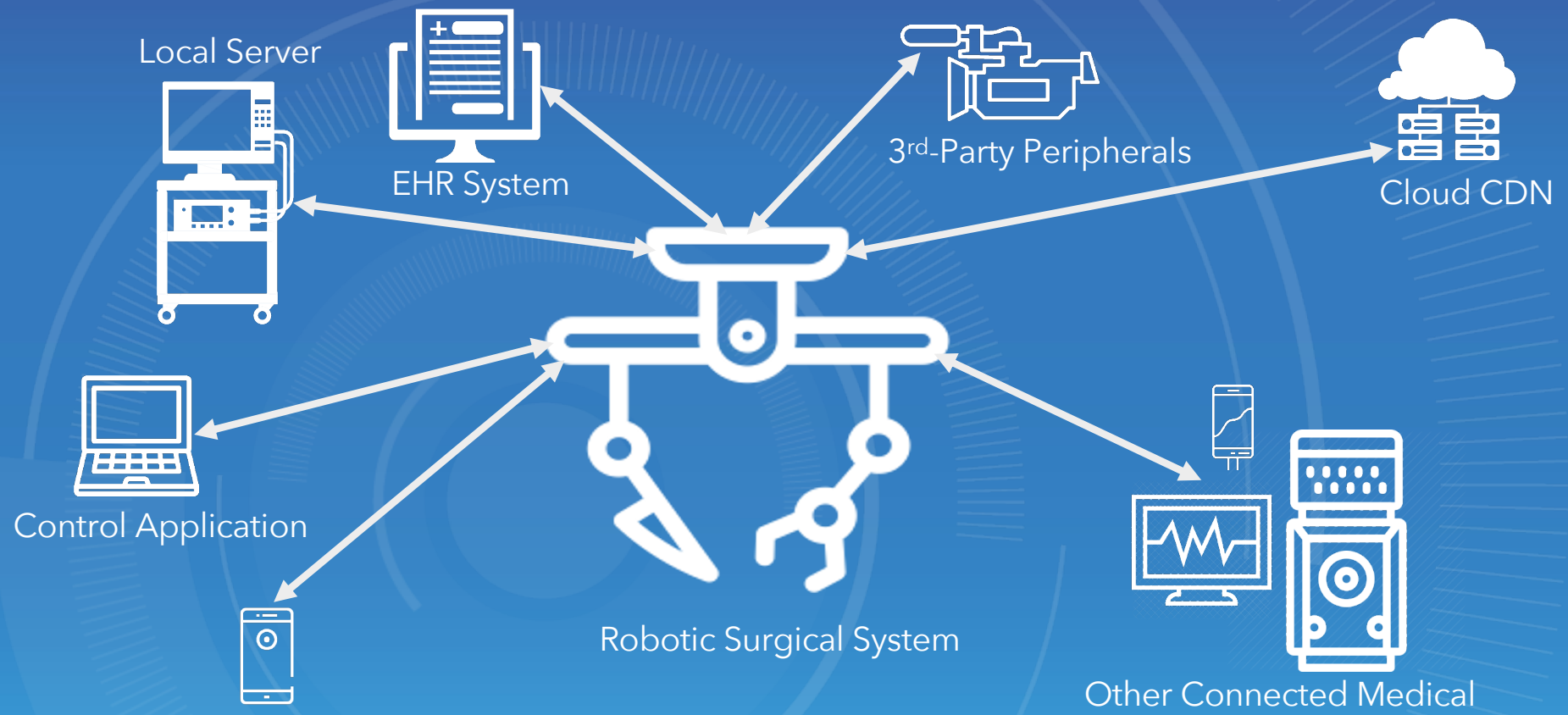
The Risk of a Vulnerability Over Time



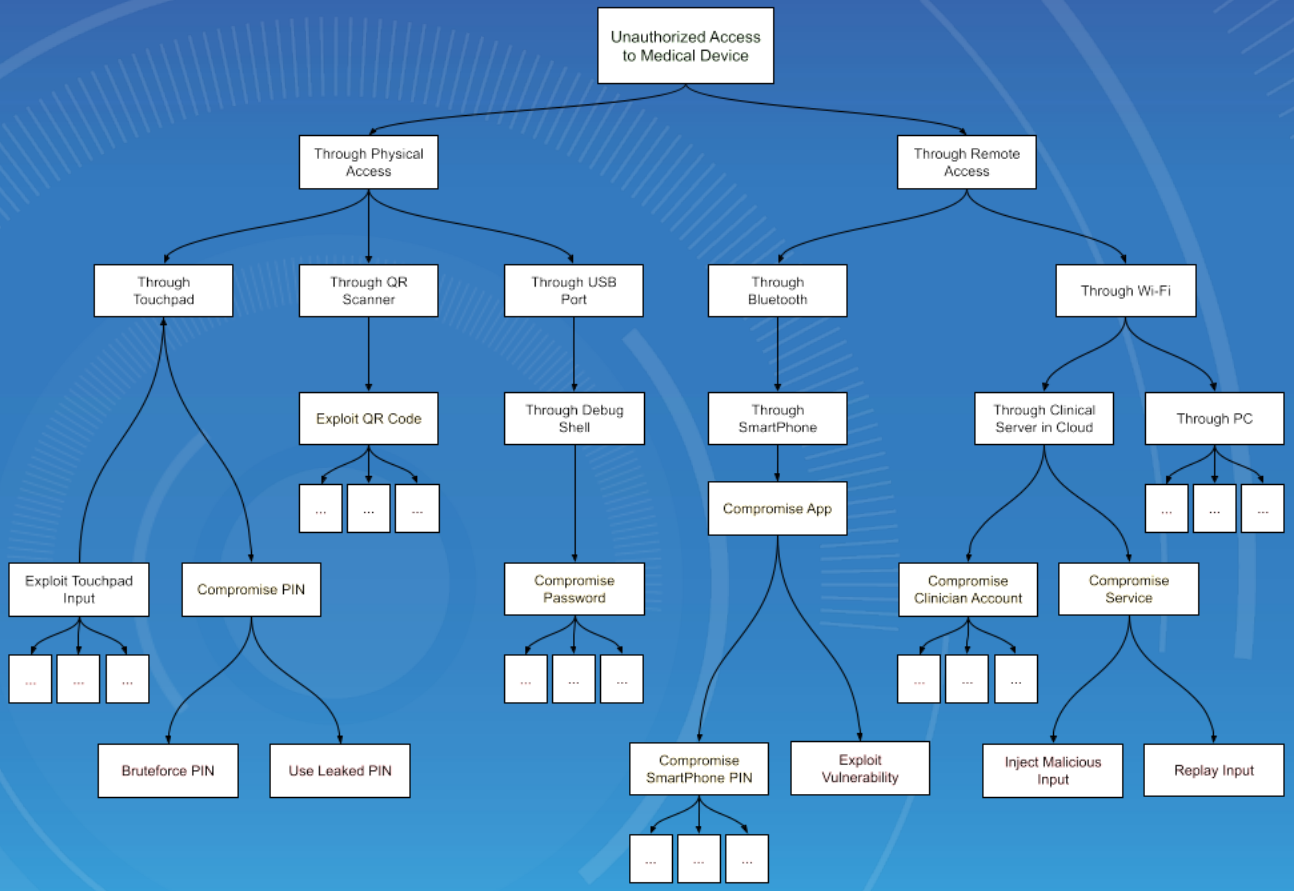
The Era of Smart Medicine

The Medical Device Attack Surface

A System of Systems



Medical Device Attack Tree



High Value Target Set

- Personal Health Information
- Billing and Insurance Data
- Intellectual Property
- Pivot Points
- Ransomware

High Risk Target Set

- Forge Patient Data
- Block Networking and Dataflows
- Disrupt or Stop Clinical Functions
- Change Dosages
- Alter Therapeutic Functions

Root access to a critical care system is the functional equivalent of having root access to the patient

Medical Device Industry
Security Motives

- Professional Responsibility and Integrity
- Corporate Reputation
- Investor Confidence
- Sales Positioning
- Competitive Pressures
- Regulatory Requirements

Regulatory Science

Technical regulatory oversight of medical systems to determine their level of cybersecurity and any potential risk to patient safety prior to receiving approval for clinical use.

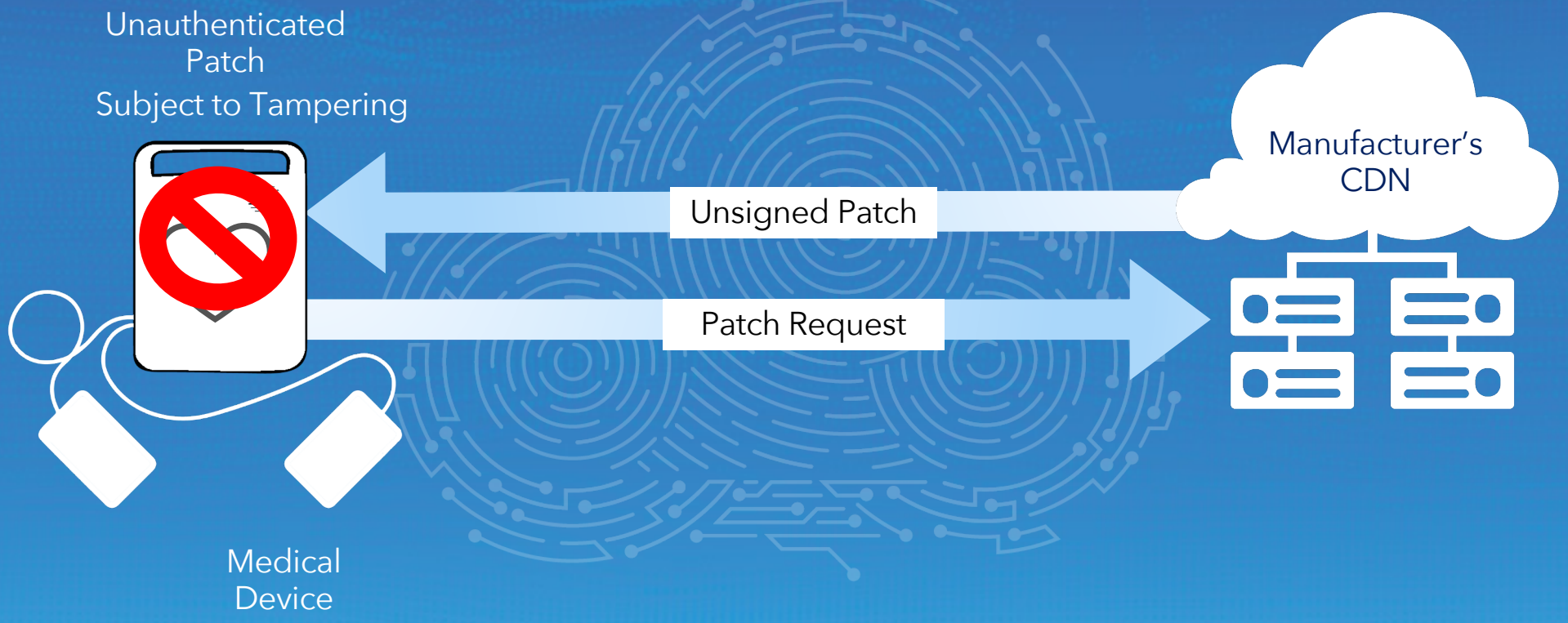
- Rigorous security review process comprising traditional cybersecurity analysis tools and methods combined with a patient safety assessment
- Typically includes an assessment of manufacturer's internal security policies, document review, pen testing, a cyberthreat assessment, and threat scoring based on a medical rubric
- Device manufactures are encouraged to have a plan in place for postmarket surveillance of new vulnerabilities

Regulatory Science

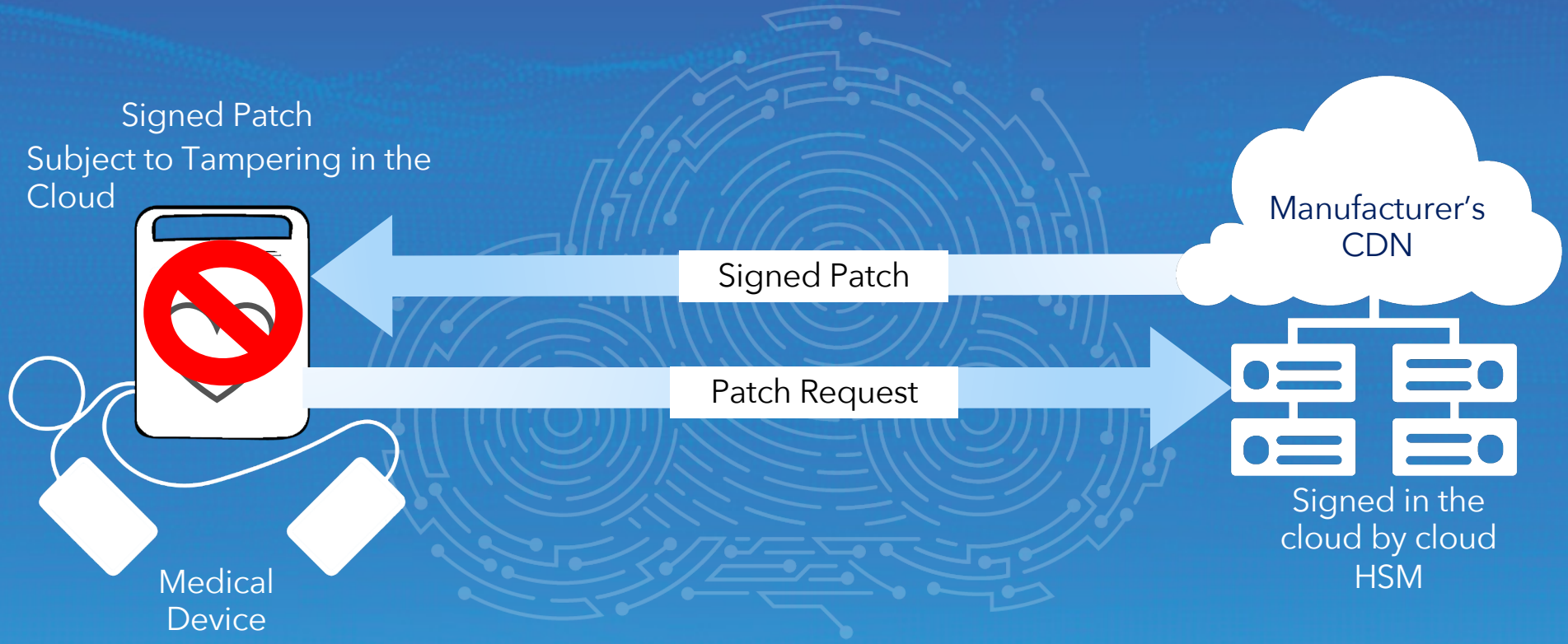
Portable Defibrillator Secure Software Patch Model

Case Study #1

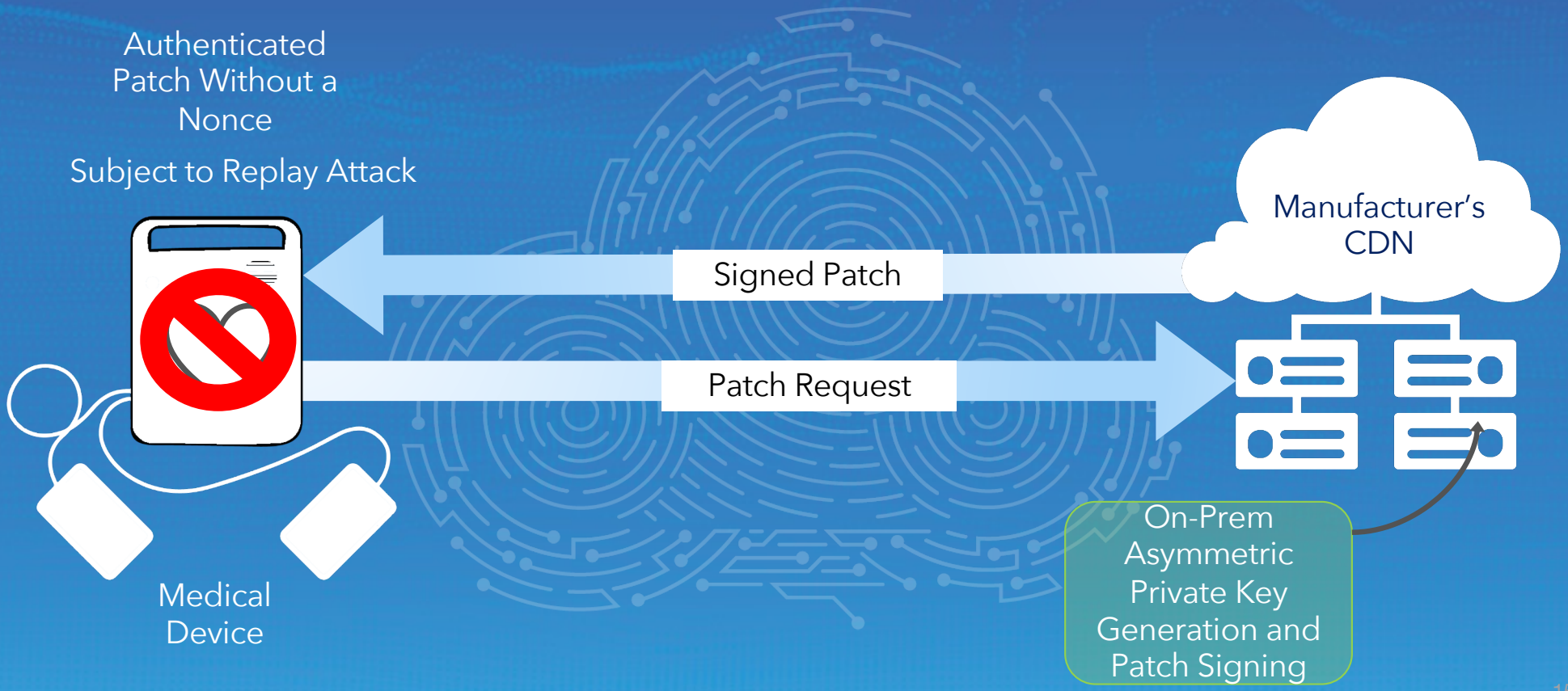
Regulatory Science
Review Process



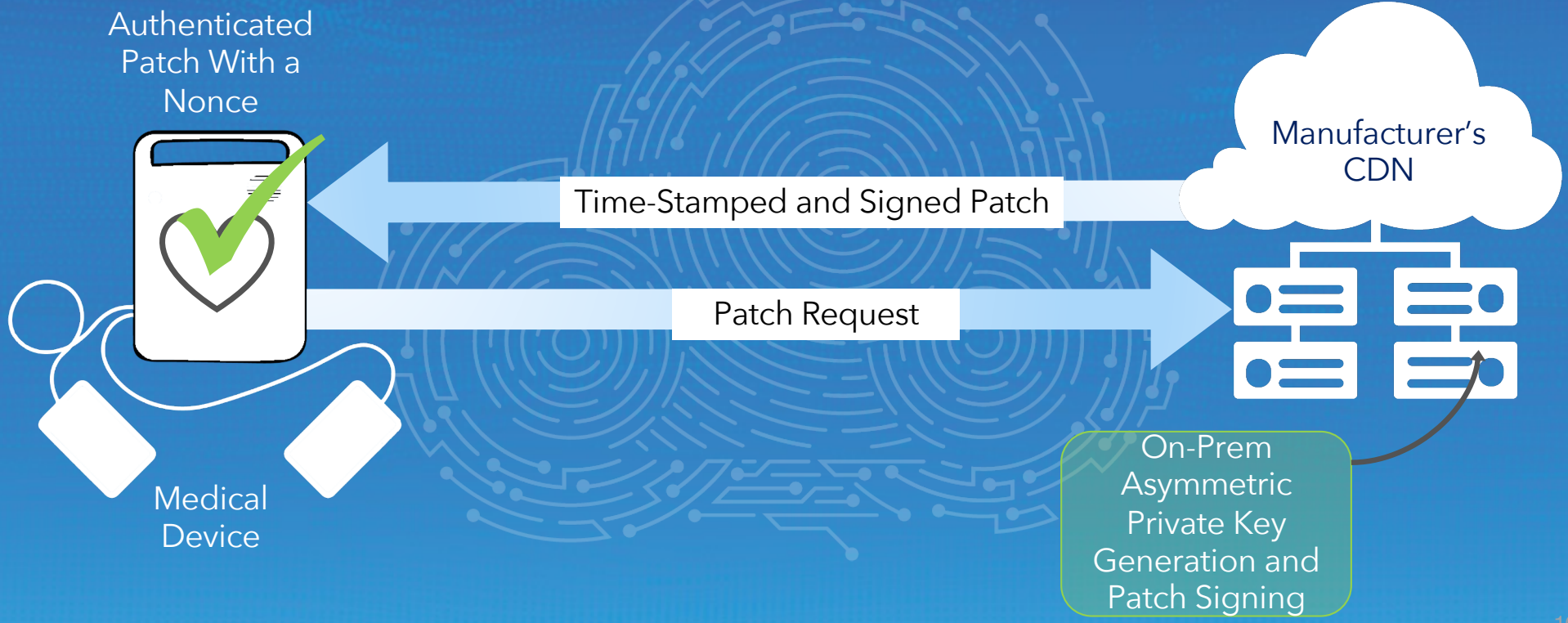
Regulatory Science
Review Process



Regulatory Science
Review Process



Regulatory Science
Review Process



Regulatory Science

Wearable Insulin Pump Secure Cloud Connectivity

Case Study #2

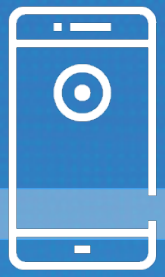
Communication Protocols

Regulatory Requirements

Pump is configurable using patient's mobile device

Data transits mobile device but cannot be accessible

Pump requires access to manufacturer's CDN through mobile device

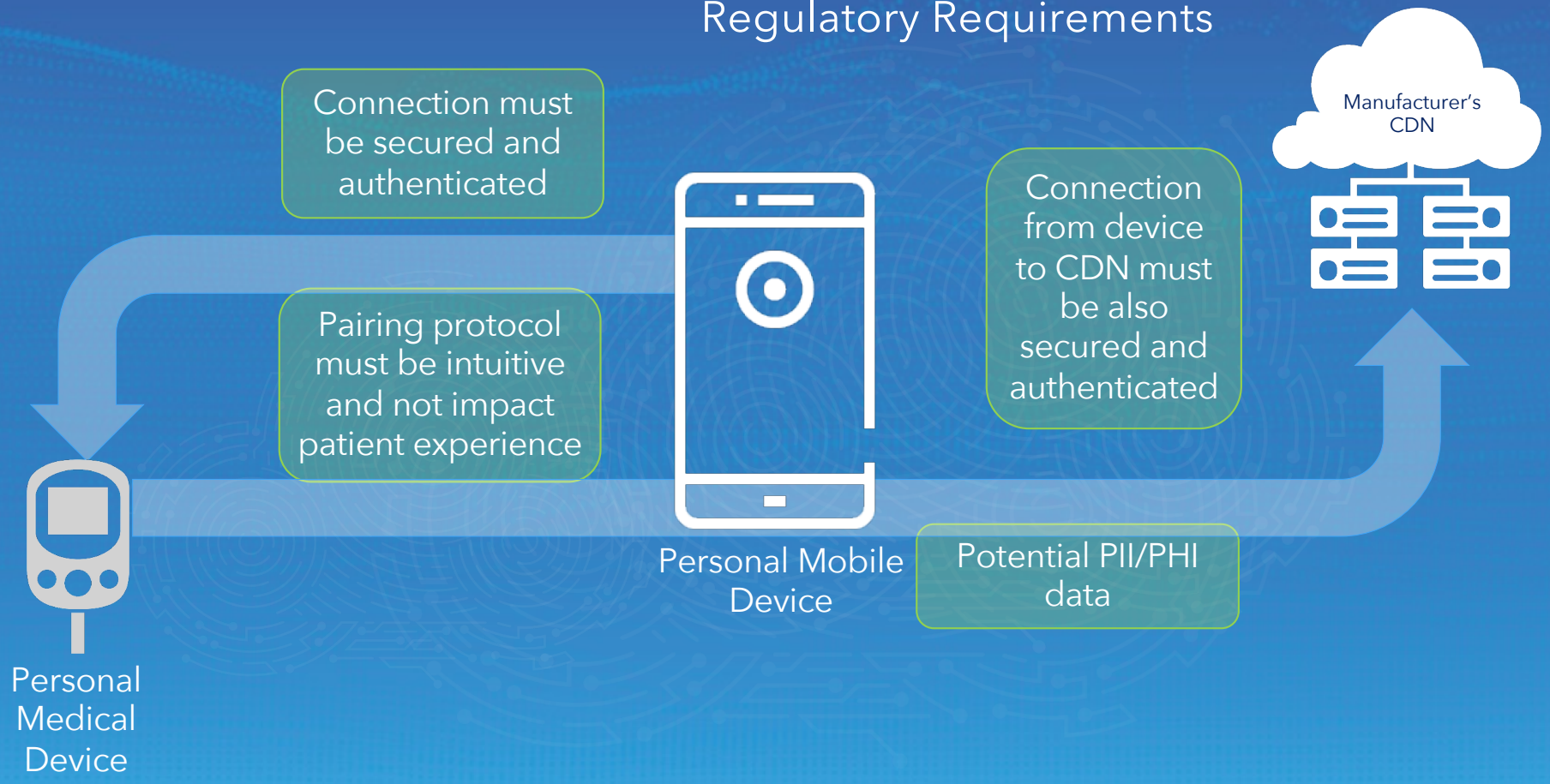


Personal Mobile Device

Personal Medical Pump

Communication Protocols

Regulatory Requirements

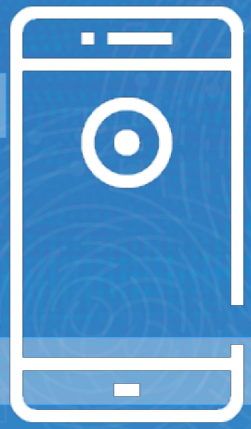


Communication Protocols

Automatically pair, authenticate and encrypt data end to end from medical device to mobile device

Regulatory Requirements

Establish end-to-end authentication and encryption from medical device to CDN



Personal Mobile Device

Personal Medical Device

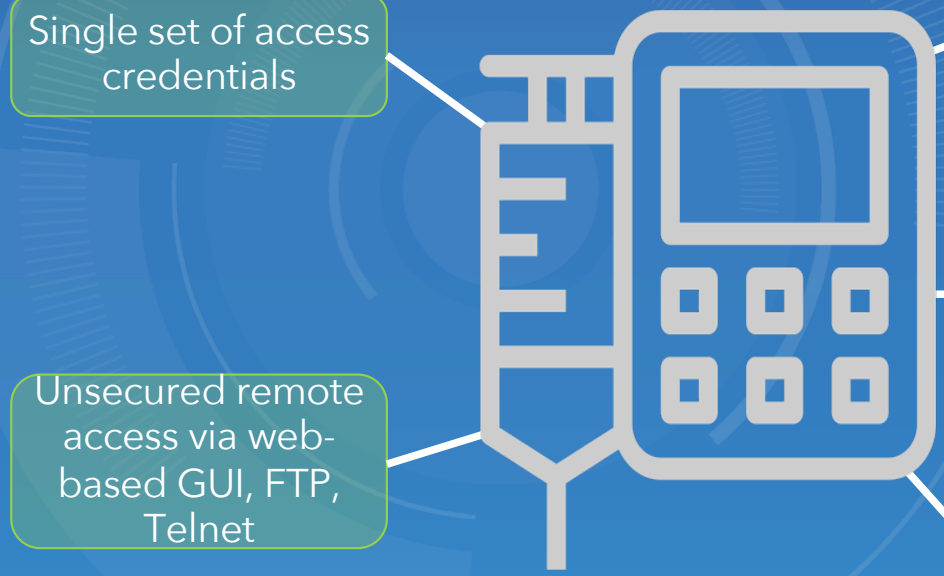
Manufacturer's CDN

Regulatory Science

Drug Infusion Pump Access Controls

Case Study #3

Access Controls

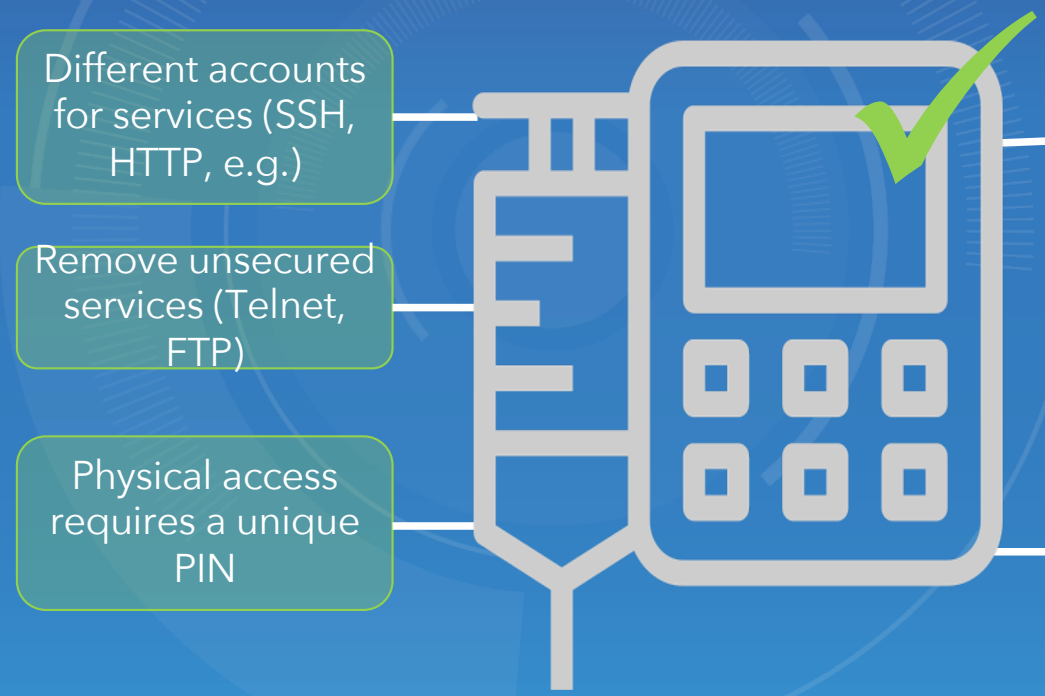


- Single set of access credentials
- Unsecured remote access via web-based GUI, FTP, Telnet
- USB port for maintenance and configuration
- Direct access to therapeutic controls via keypad
- Clinical mode and maintenance mode operate simultaneously

Access Controls

- No differentiation between users
- USB port allowed unauthenticated access to file system
- Open ports create remote access vulnerabilities
- If resources fail while in maintenance mode, clinical operations could be impacted

Access Controls



- Different accounts for services (SSH, HTTP, e.g.)
- Remove unsecured services (Telnet, FTP)
- Physical access requires a unique PIN
- Communications functions and clinical operations partitioned by hardware resources and OS
- Clinical mode is disabled whenever the device enters into maintenance mode

Risk Mitigation

- Aided by attack trees
- Must define the threat model
- Process is not fully automated
  - You have to be smart and think
- Similar thought process applies to other domains
  - Banking
  - Transportation
  - Communications
- Consider the threats that are specific to your application

Medical Device Safety
Now and Future

- Medical devices are becoming more complex, more technically diverse, more connected, and more personal
- A category of security professionals is emerging that combines a knowledge of medical technologies and regulatory requirements with an advanced cybersecurity skill set
- The current state of medical device safety is the result of industry foresight and diligence, not decreasing danger and risk
- The unique status of medical devices will demand that they continue receive the energy and resources necessary to ensure their cybersafety

harborlabs™
CYBER . SCIENCE

Thank you!

Avi Rubin

rubin@harborlabs.com

@avirubin

https://www.linkedin.com/in/avirubin/