ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

2023 ACCE CE-IT Symposium

Securing IoMT Proactively

Collaboration Between Information Technology and Clinical Engineering Profession

Medical Device Security
Why it is so hard, and what can you do about it?

Phil Englert

Director of Medical Device Security

HEALTH-ISAC

Health-ISAC™
Collaborating for Resilience in Healthcare

Phil Englert

Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

About the Speaker

Phil is the VP Medical Device Security for Health-ISAC, working with Medical Device Manufacturers (MDMs) to help improve privacy and security while coordinating with Health Delivery Organizations (HDOs) to ensure implementations are practical and achievable. Phil is a subject matter expert and contributor to Health-ISAC's Medical Device Security Information Sharing Council (MDSISC). He has over 30 years of technical and operational leadership experience in healthcare and life sciences,. Previous positions include Chief Product Officer at Medsec, Global Leader for Medical Device Technology at Deloitte, Vice President of Operations at MDISS, and National Director of Technology Operations at Catholic Health Initiatives.

Session Description

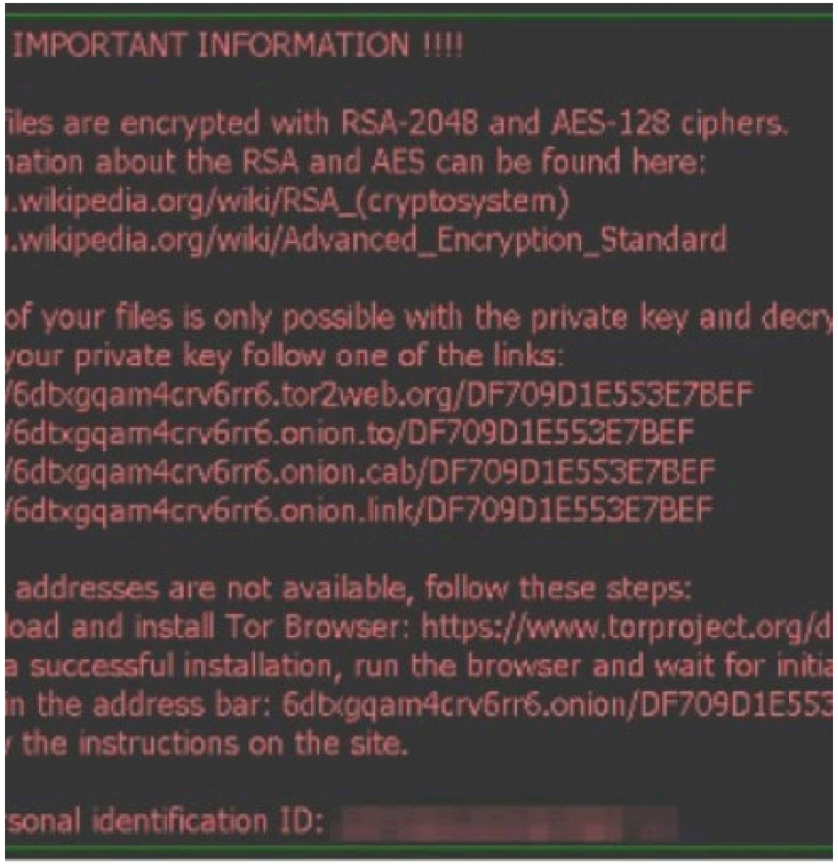
The spectrum of technologies supporting health care is staggering, and medical devices are a large part of the complex ecosystem delivering patient care. The things medical devices enable caregivers to do is genuinely awe-inspiring.

This diversity of technology is also more connected than ever before. Healthcare is an information business, and medical device technology generates much of the data supporting patient care. The burden of ensuring this technology remains safe to use, protects patient data, and is available when needed, falls squarely on the shoulders of HTM staff. As bad actors crank up attacks on healthcare, HTM staff increasingly take on cybersecurity responsibility. This extra duty may seem daunting, but HTM staff are more prepared than they realize.

This session will discuss the challenges of securing medical devices and what HTM staff can do to reduce the threat surface, limit the blast radius, and improve the efficiency and effectiveness of response and recovery activities for their organization.

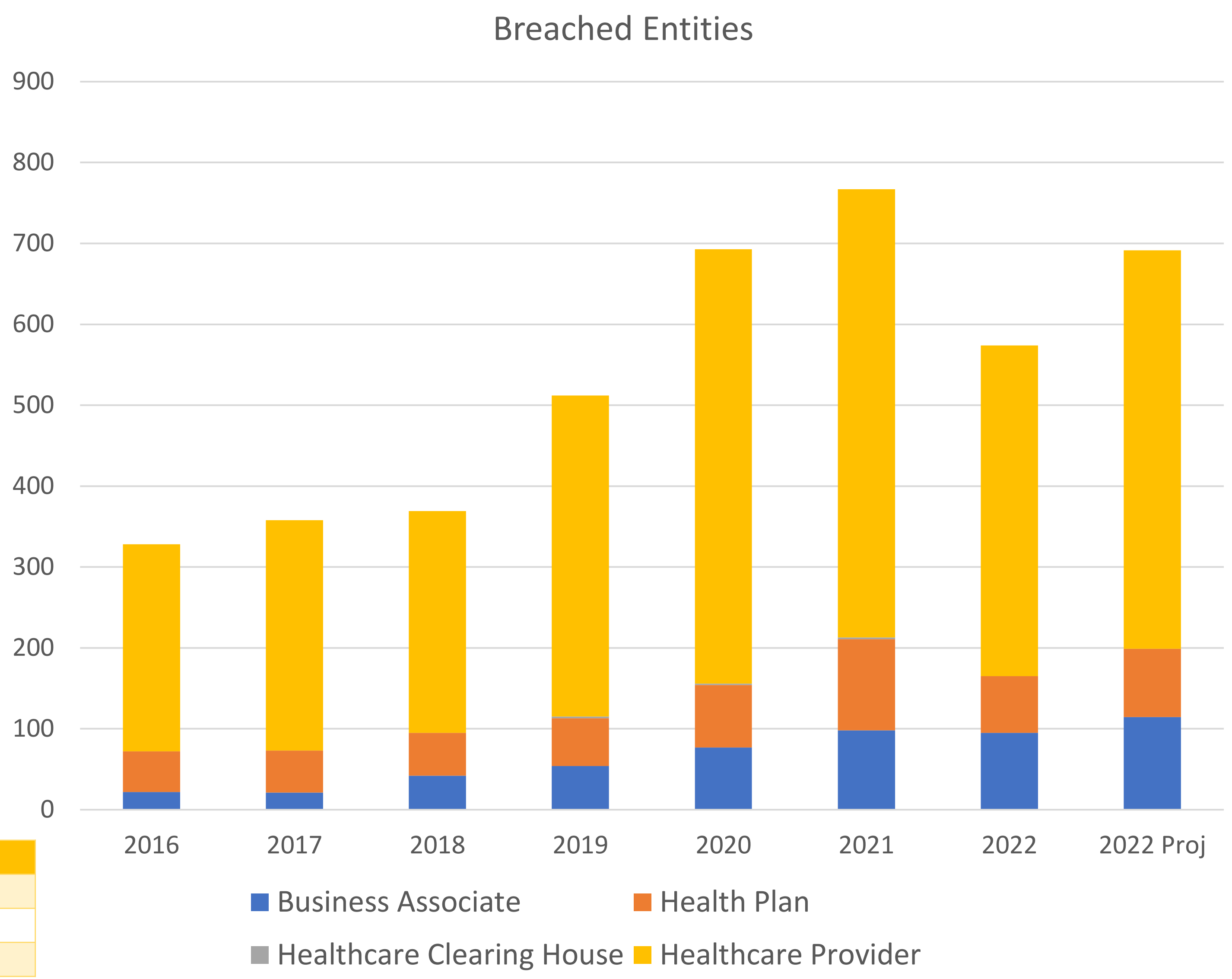
Healthcare is under attack

- Hollywood Presbyterian Medical Center
- 434 bed Level II trauma center serving a multicultural urban LA community
- Feb. 5, 2016 – staff reported inability to access records
- Internal emergency declared
- Record access/sharing not possible
- Patients diverted
- FBI & local Law enforcement called in
- 40 bitcoin ($17,000) already paid
- Recovery declared on February 15th
- Locky ransomware spread via MS Word



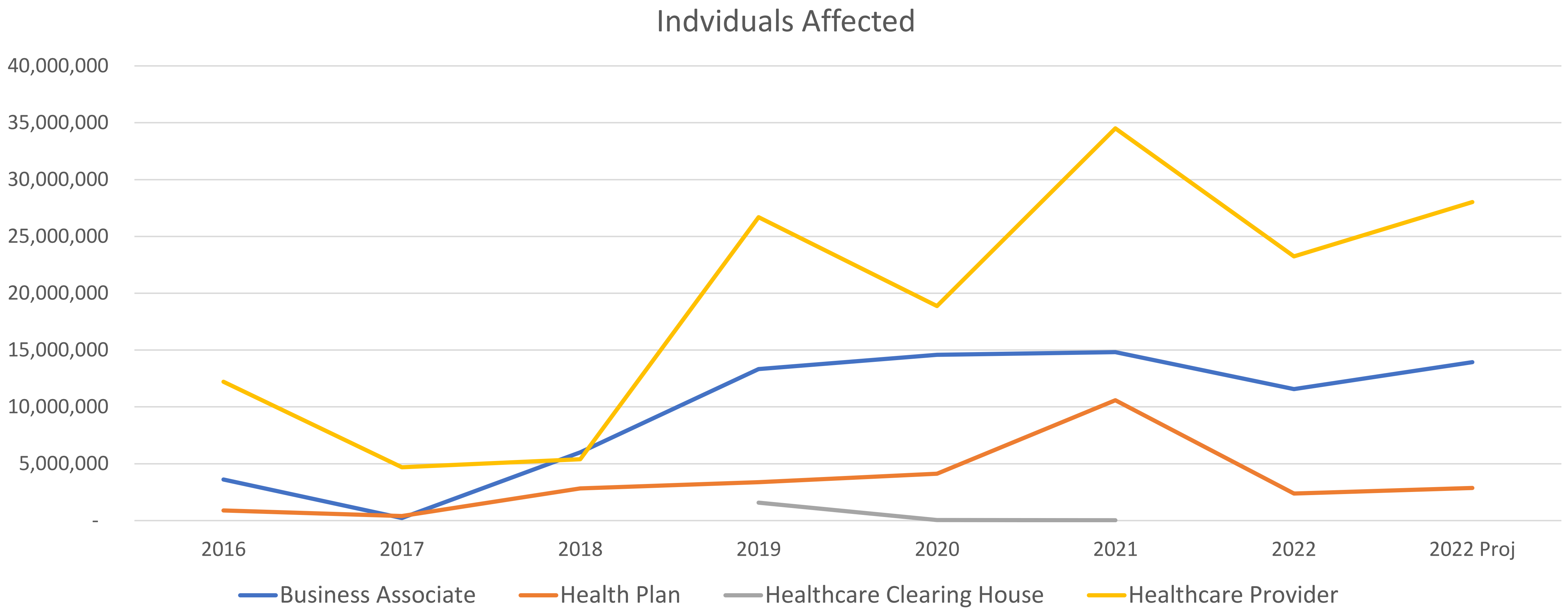
```
IMPORTANT INFORMATION !!!!

iles are encrypted with RSA-2048 and AES-128 ciphers.
nation about the RSA and AES can be found here:
.wikipedia.org/wiki/RSA_(cryptosystem)
.wikipedia.org/wiki/Advanced_Encryption_Standard

of your files is only possible with the private key and decry
your private key follow one of the links:
/6dtxgqam4crv6rr6.tor2web.org/DF709D1E553E7BEF
/6dtxgqam4crv6rr6.onion.to/DF709D1E553E7BEF
/6dtxgqam4crv6rr6.onion.cab/DF709D1E553E7BEF
/6dtxgqam4crv6rr6.onion.link/DF709D1E553E7BEF

addresses are not available, follow these steps:
load and install Tor Browser: https://www.torproject.org/d
a successful installation, run the browser and wait for initia
in the address bar: 6dtxgqam4crv6rr6.onion/DF709D1E553
the instructions on the site.

sonal identification ID: [redacted]
```

Breach count by entity type



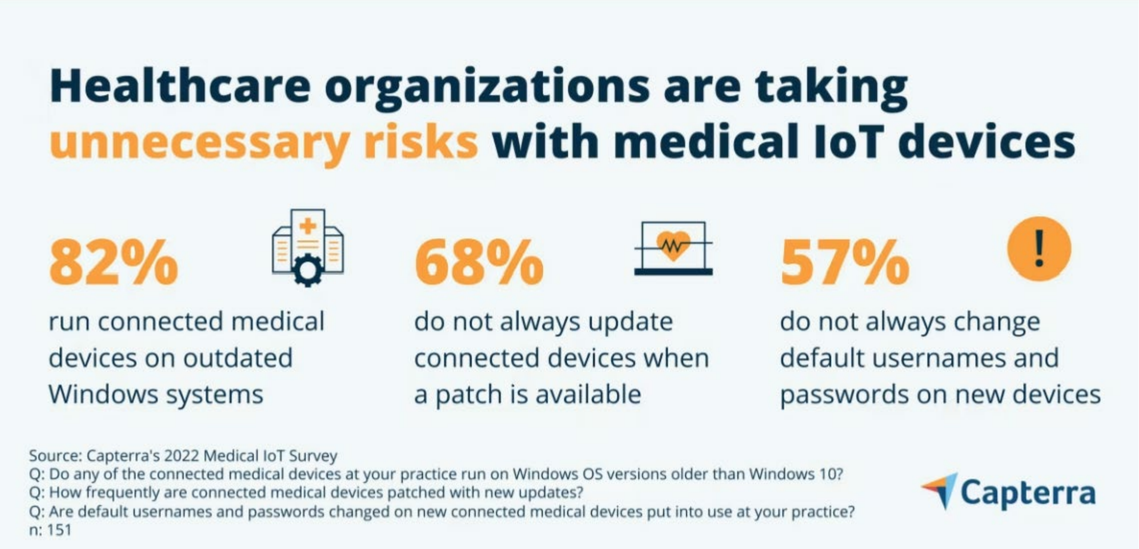
Year	Avg $/breach	Breaches	Healthcare Impact
2021	$ 9,300,000	554	$ 5,152,200,000
2020	$ 7,130,000	537	$ 3,828,810,000
2019	$ 8,000,000	397	$ 3,176,000,000

Individual records by entity type



Survey Says!

- Healthcare organizations with a higher percentage of connected medical devices suffer more cyberattacks.



Healthcare organizations are taking unnecessary risks with medical IoT devices

82% run connected medical devices on outdated Windows systems

68% do not always update connected devices when a patch is available

57% do not always change default usernames and passwords on new devices

Source: Capterra's 2022 Medical IoT Survey
Q: Do any of the connected medical devices at your practice run on Windows OS versions older than Windows 10?
Q: How frequently are connected medical devices patched with new updates?
Q: Are default usernames and passwords changed on new connected medical devices put into use at your practice?
n: 151

- Nearly half (48%) of healthcare cyberattacks impact patient care, and two in three (67%) affect patient data.
- More than half (53%) of healthcare IT staff view the current cybersecurity threat landscape as high or extreme.
- Less than half (43%) of practices say they always change default passwords on connected medical devices, and less than a third (32%) always update them when a patch is available.

https://www.capterra.com/resources/medical-internet-of-things-iot-security/

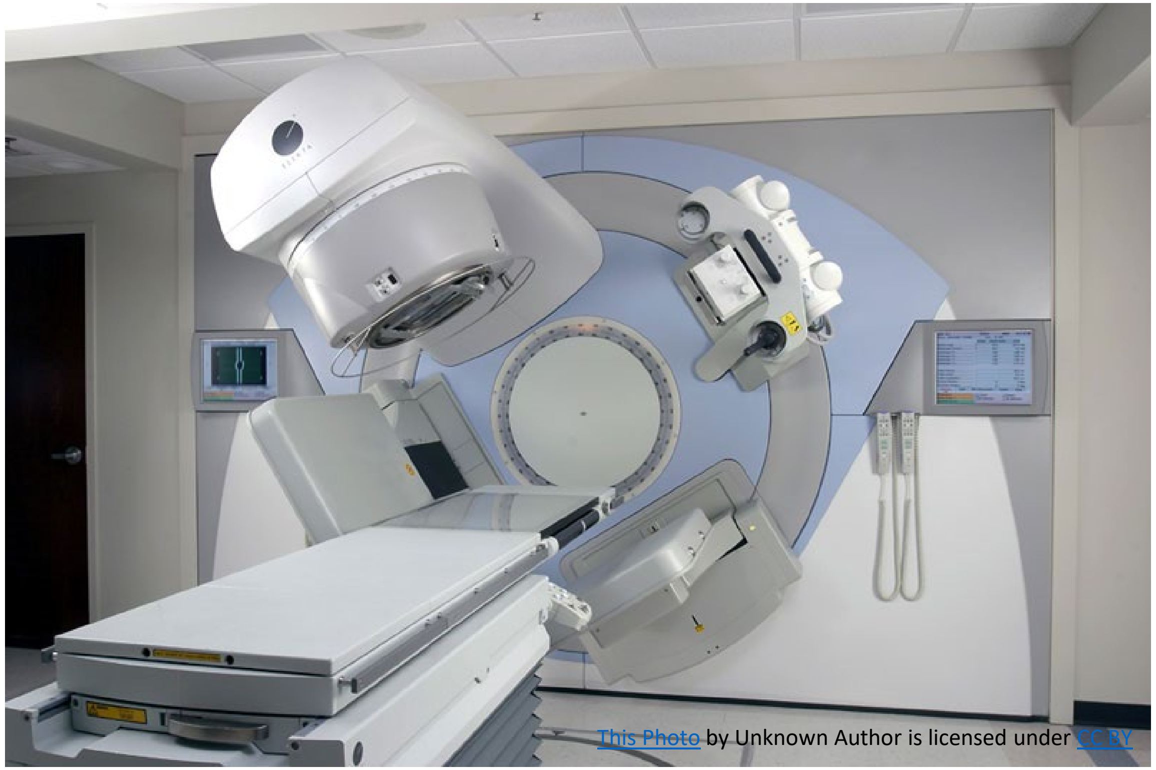
A woman dies during a cyber-attack on a hospital

- September 10, 2020
- Düsseldorf University Hospital
- Russian based hackers - "Doppelpaymer“
- 78-year-old woman suffering from an aortic aneurysm
- 30 Servers – hospital on divert – connection to ambulance severed
- Diverted 32Km (~20m) delaying treatment by more than 1 hour
- 1st ever reported death attributed to cyberattack
- Negligent-homicide investigation

Medical Devices and IoT

1. Purpose built devices for hundreds of purposes
2. Designed for precision and reliability
3. Technology debt – life cycle disparity
4. Lack of manufacturer transparency
5. Software as a Medical Device

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY

Medical Modalities

1. Imaging
2. Monitoring
3. Therapeutic
4. Diagnostic
5. General

IoT Modalities

1. Environmental Monitoring
2. Utilities
3. Life Safety
4. Access Control
5. Transport

FDA observed medical device vulnerabilities

- Network-connected medical devices infected or disabled by malware
- Malware on hospital computers, smartphones/tablets, and other wireless mobile devices used to access patient data, monitoring systems, and implanted patient devices
- Uncontrolled distribution of passwords
- Failure to provide timely security software updates and patches
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access

Why is this so hard?

Security incidents will grow as IoMT technology advancement accelerates

2019: Implanted defibrillators telemetry protocol flaw

Some implanted defibrillators were found to contain vulnerabilities that would allow them exploited by attackers who had the right knowledge of the devices and close proximity to an individual possessing one.

2016: Insulin pumps remotely exploitable

Rapid7 and Johnson & Johnson disclosed three vulnerabilities in an insulin pump system that could be remotely exploited.

2018: Poor security on PACS systems

PACS (picture archiving and communication system) are used for picture archiving and communication system. Security researchers found several vulnerabilities both in commercial and open-source PACS.

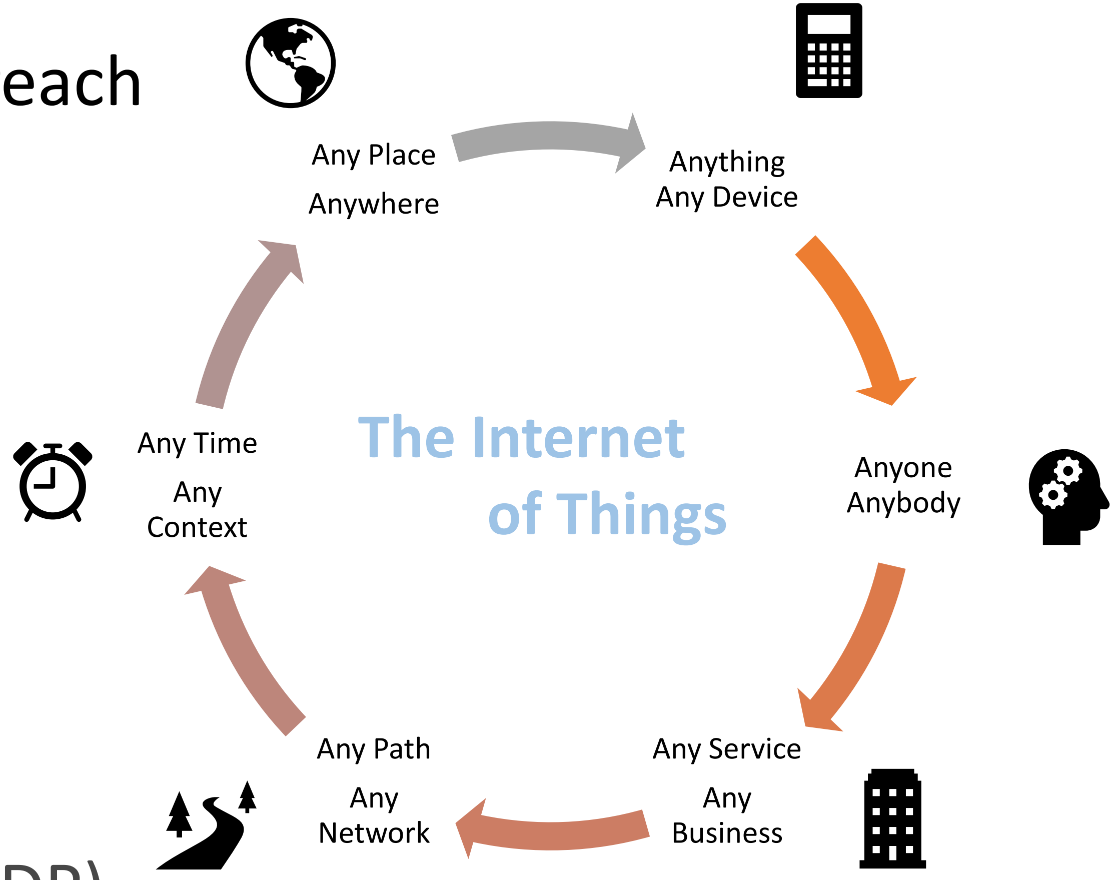
2014: Anaesthesia delivery system bugs.

The anaesthesia delivery system is used in hospitals to deliver oxygen, anaesthetic vapor, and nitrous oxide to during surgical procedures. Software bugs were found so serious that they could cause severe injury or death, even just plugging a phone into the USB port.

Securing medical devices in a increasingly connected world, Andy Bridden, 1/21/20

Internet of Things

- Global IoT spending is expected to reach $1t in 2023
- 7b IoT devices
  - 3x to 24b by 2030
- US medical device manufacturing revenue $50b in 2023
- 3.4% growth rate
- US healthcare expenditure
  - $4.3t in 2021 ($12,914/person)
- 16.8% of gross domestic product (GDP) in 2019



The Internet of Things

Any Place
Anywhere

Anything
Any Device

Anyone
Anybody

Any Service
Any
Business

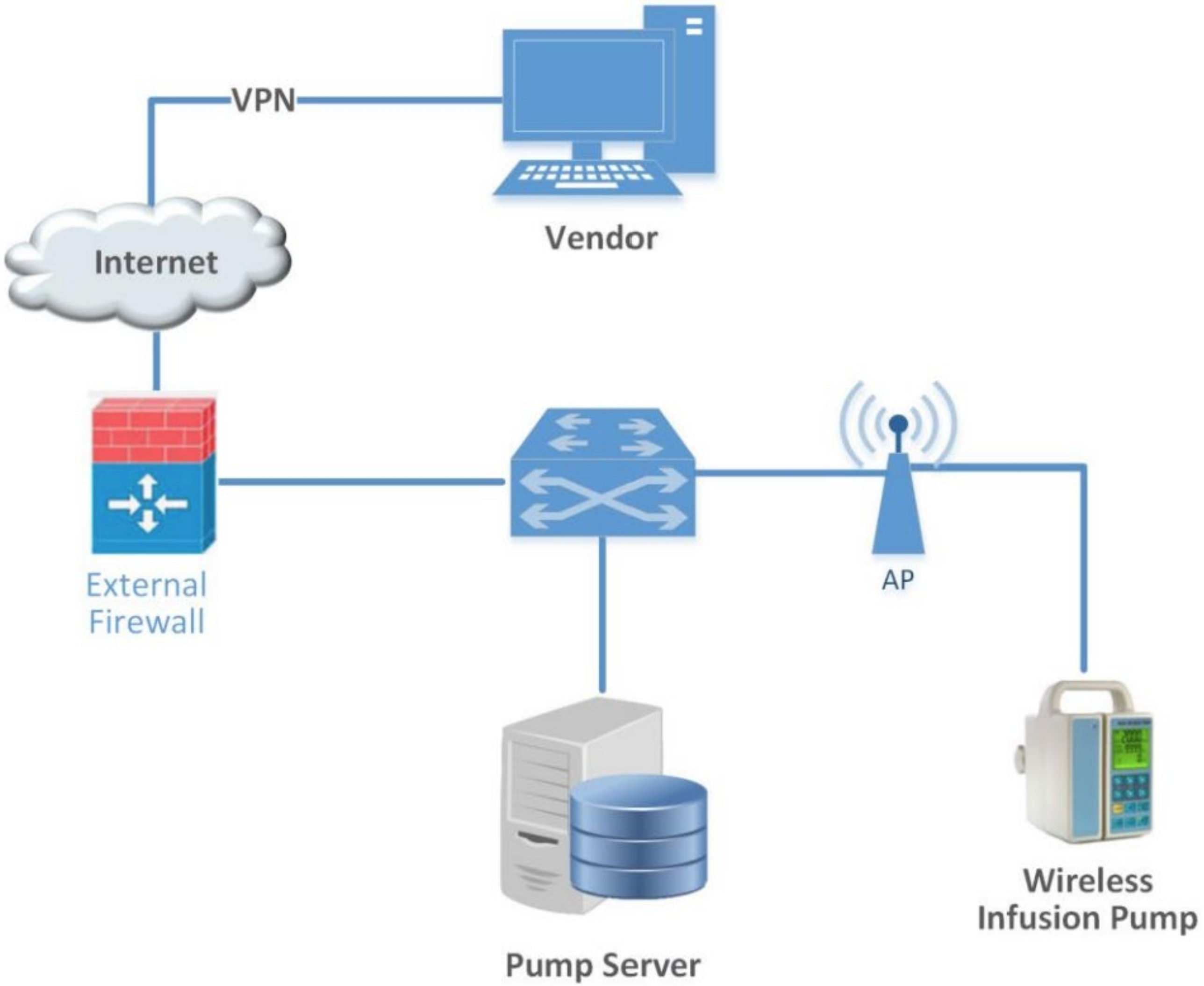
Any Path
Any
Network

Any Time
Any
Context

https://www.insiderintelligence.com/insights/healthcare-industry/
https://www.ibisworld.com/industry-statistics/market-size/medical-device-manufacturing-united-states/#:~:text=The%20market%20size%2C%20measured%20by,is%20%2450.8bn%20in%202023.

Basic infusion pump management system

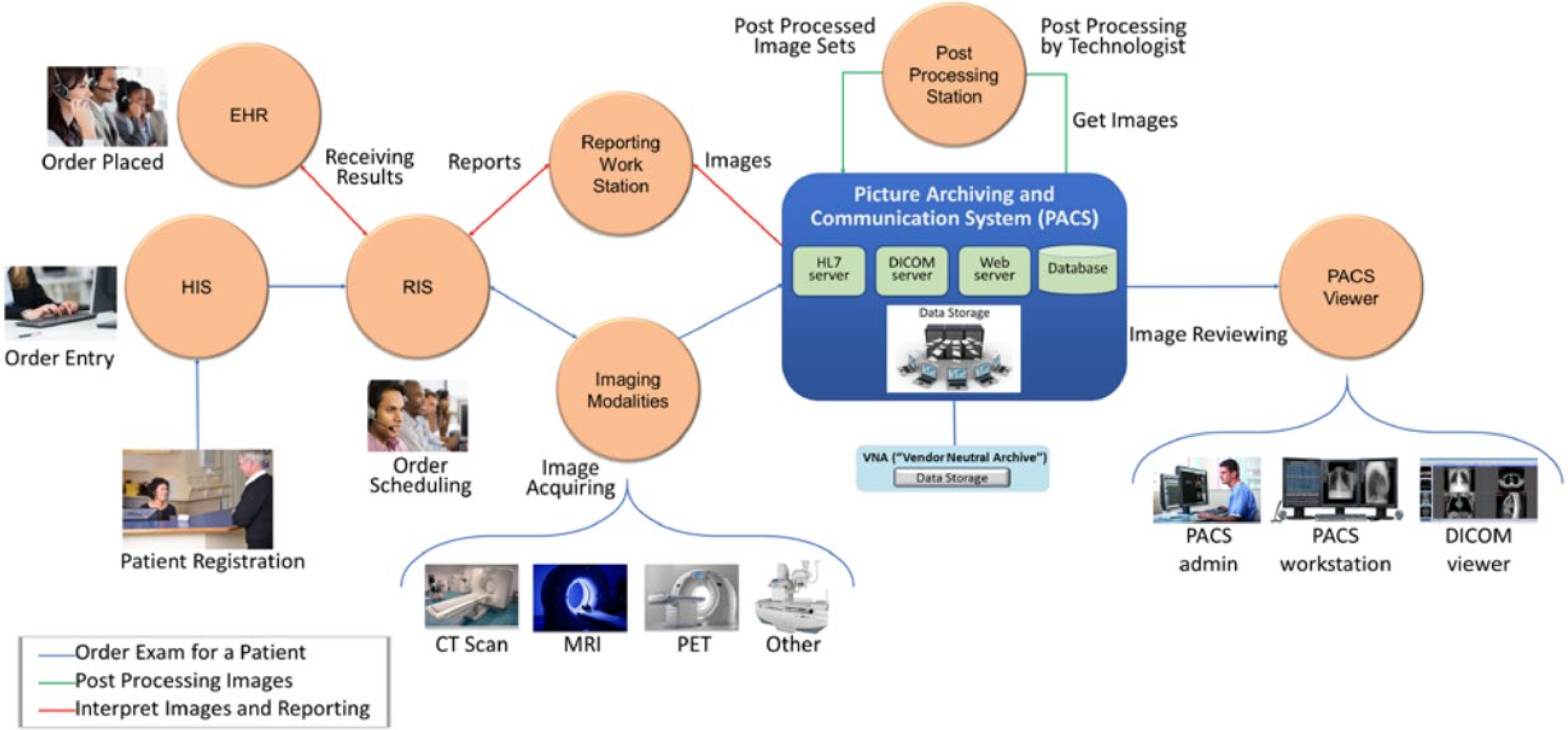
Figure 5-1 Basic System



NIST.S.P.1800-8 Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

Sample diagnostic imaging system

Figure 3-2 Scenario One: Sample Radiology Practice Workflows



NIST.SP.1800-24 Securing PACS

Telehealth Remote Patient Monitoring system

Figure 4-1 RPM Architecture

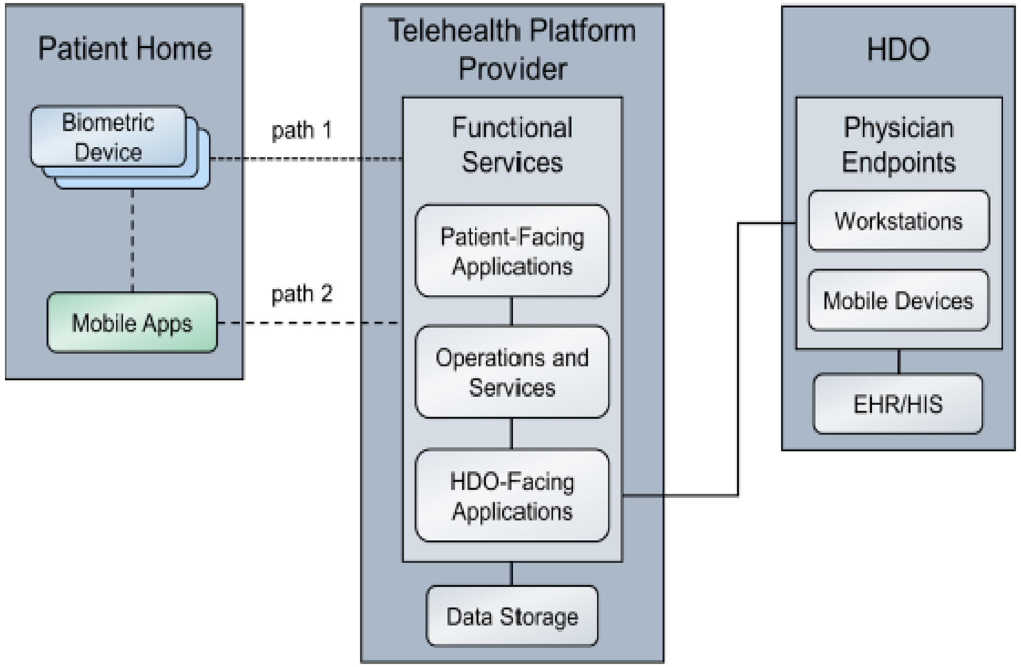
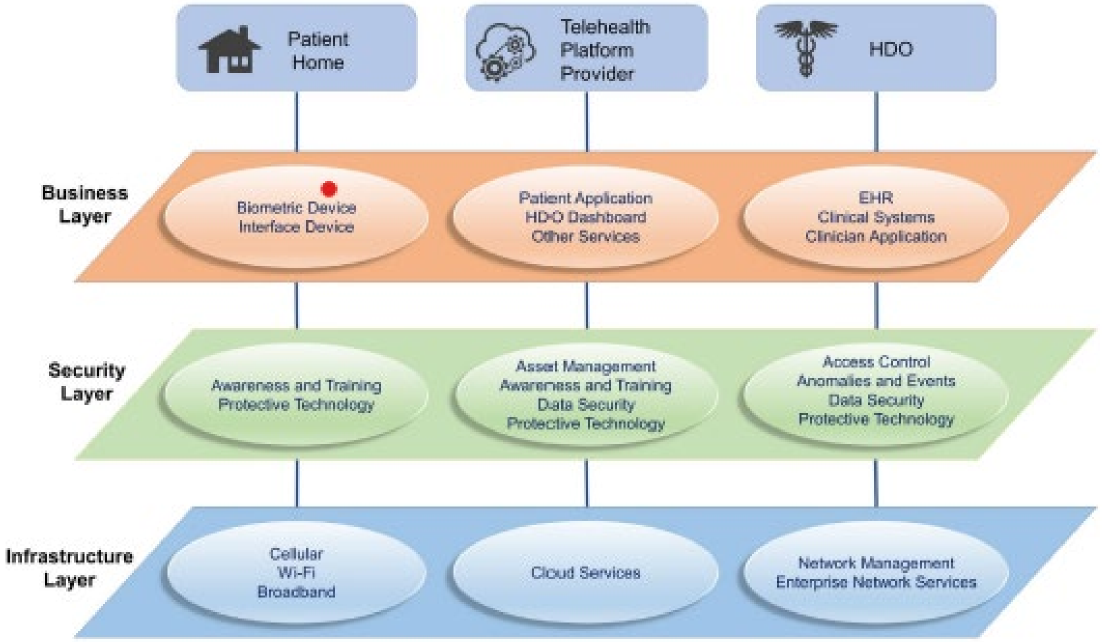


Figure 4-2 Architecture Layers



Patient Home
Telehealth Platform Provider
HDO
Business Layer
Biometric Device Interface Device
Patient Application HDO Dashboard Other Services
EHR Clinical Systems Clinician Application
Security Layer
Awareness and Training Protective Technology
Asset Management Awareness and Training Data Security Protective Technology
Access Control Anomalies and Events Data Security Protective Technology
Infrastructure Layer
Cellular Wi-Fi Broadband
Cloud Services
Network Management Enterprise Network Services

NIST.S.P.1800-30A Securing Telehealth Remote Patient Monitoring Ecosystem

Healthcare matrix

- 6,400 acute care hospitals
- Urban, teaching or trauma
- Suburban & community
- Rural & critical access

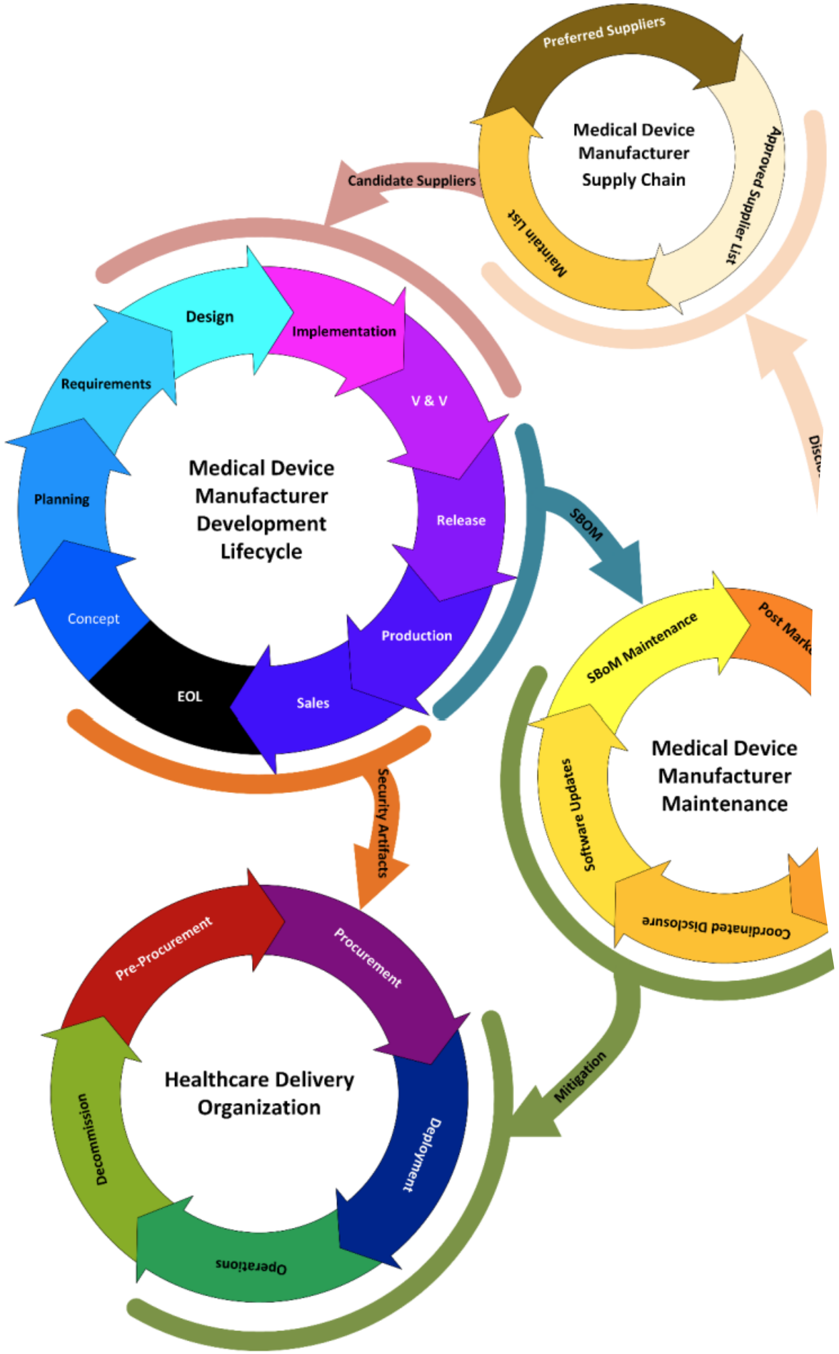
- ↑400 ancillary care locations each
- Diagnostic & surgery centers
- Clinics, wellness, & pharmacy
- Physician practices

- FDA
  - 6,750+ Product Codes
  - ~530 connectable
  - ~100 clinical functions
- 380,000+ medical devices
- Approximately 100k connectable
- 1,200 makes and models
- 350+ manufacturers

- ~20 manufacturers account for 80% of device count in an acute care setting

Hospital ransomware attack allegedly led to infant's death

- Springhill Medical Center
- July 2019 - > 3 weeks
- Mother not informed during admission (8 days into the attack) for a scheduled labor induction
- Fetal distress not detected, Emergency C-section
- 1st confirmed death pending court decision



ure 1: Main Areas and Phases of Lifecycle Management

Complex Lifecycle Management

- Breadth of technologies
- Legacy devices
- Variety of care delivery environments
- Multiple responsible parties
- Dilution of priorities
- Regulatory uncertainty

What can you do about it?

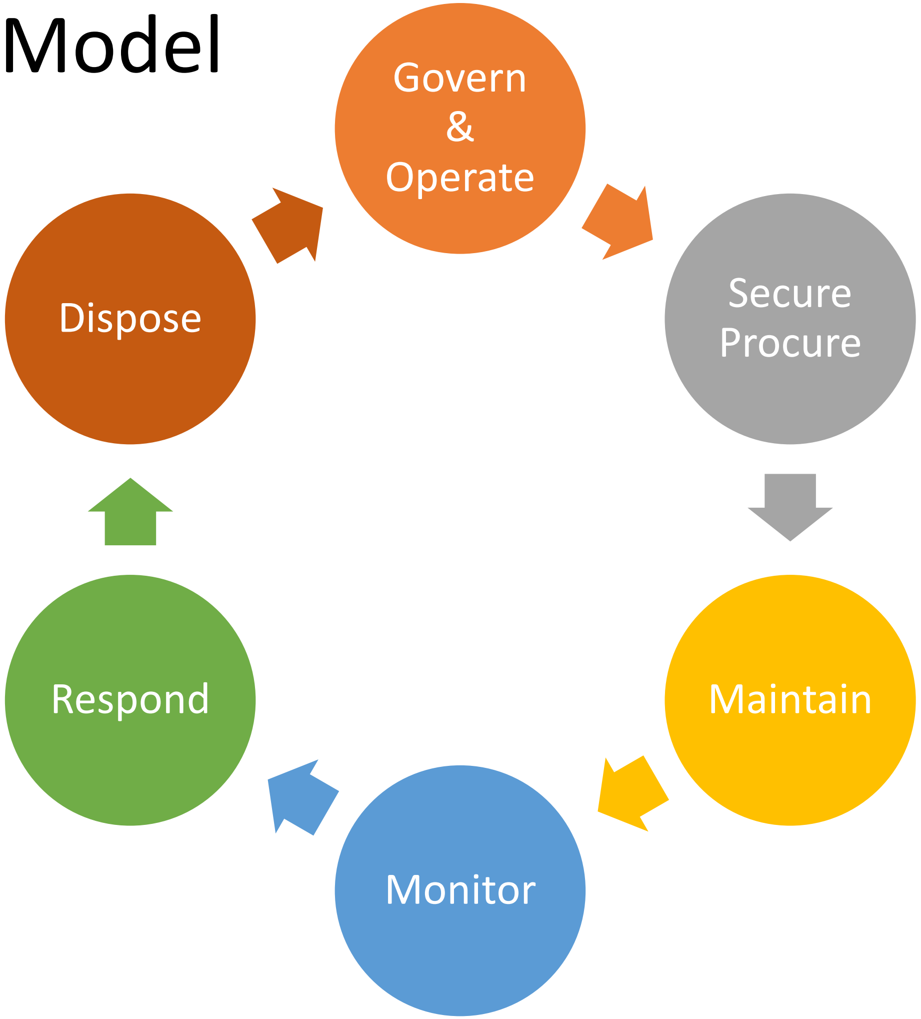
You know what to do

✓ HTM JOB #1 IS MAINTENANCE OPERATIONS

⚠ CYBER IS A FAILURE MODE

! PREPARE AND RESPOND

- Governance & Operating Model
- Secure Procure
- Maintain
- Monitor
- Respond
- Dispose



Program Elements

Governance and Operating Model

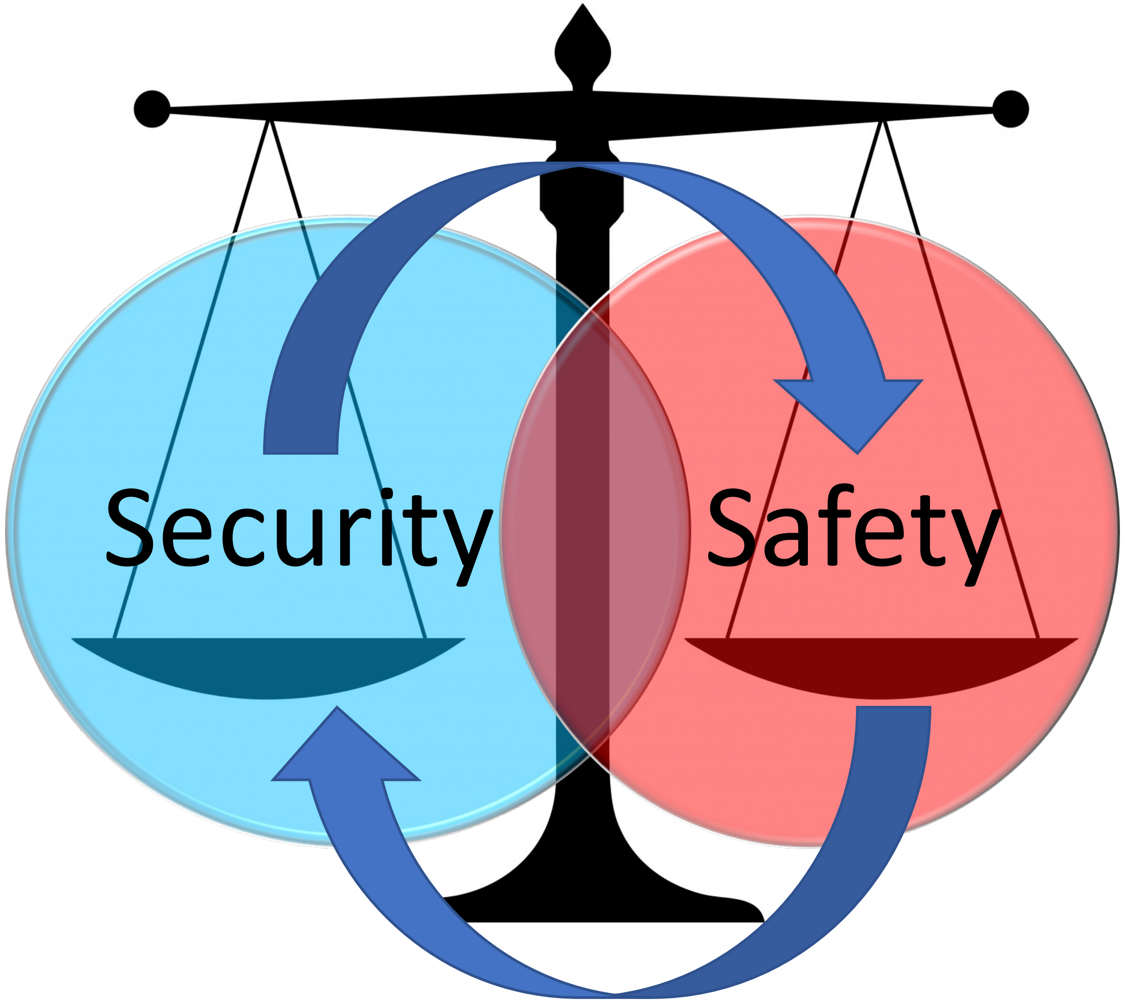
- Governance
  - Who makes what decisions
    - Environment of Care
      - Regulatory requirements
      - Risk Management
      - Patient Safety
    - Performance Improvement Plans
    - Spending authority
    - Data Protection
    - Staff Management
    - Education & Training

- Operating Model
  Medical Equipment Management Plan (MEMP)
    - Equipment inventory
    - Program performance monitoring and reporting
    - Equipment maintenance program
    - Incident monitoring and reporting
    - Equipment failure response
    - Response to product notices and recalls

Risk Management

- HTM keeps it running
- IT keeps it talking
- Safety changes may impact security
- Security changes may impact safety
- Not just failure, there is intent

- **Business owner decision**



Asset Management

IT	HTM
Standards compliance	Install base alignment
Risk assessment	Incoming Inspection
IP address, MAC address	Asset ID, RTLS tag
OS & patch level, components	Make, model, version
Vulnerability scanning	Passive scanning

ACCE – 2023 CE-IT Symposium

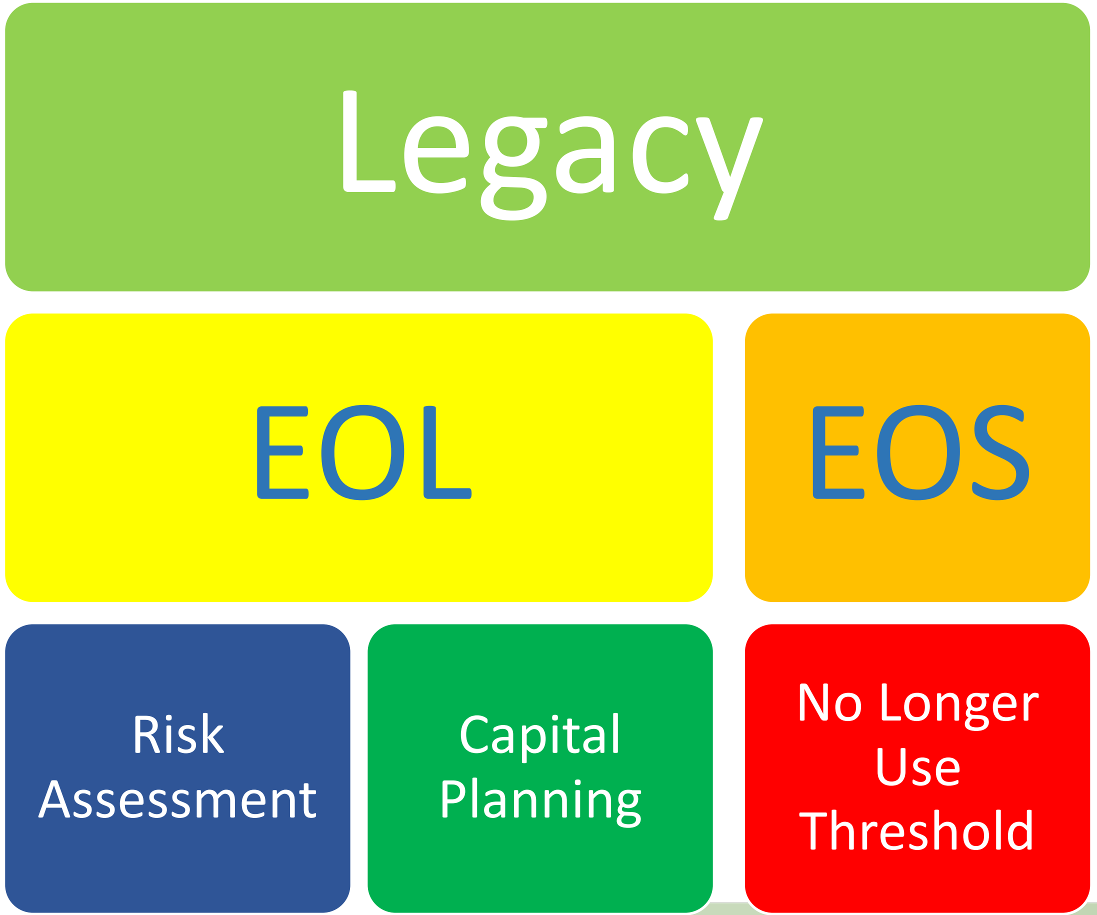
Secure Procurement

Evaluation of fit through multiple stakeholder lenses

- **Clinical benefits**
  - More procedures or procedure types
  - Staff efficiencies and satisfaction
- **Finance**
  - Increased revenues
  - Decreased costs
- **Serviceability**
  - Reliability
  - Service strategy
- **Risk Management**
  - Safe to use
  - Secure to operate
  - Future proof

Legacy Equipment

- AHA Useful life - 7-12 years
- OS is out of support
- Manufacturer no longer supports
- Bailing wire and bubblegum
- Clinically useful
- A backup
- End of Life/Support
    - Risk assessment
    - Support costs
    - Capital planning
    - **No Longer Use Threshold**



Legacy

EOL

EOS

Risk Assessment

Capital Planning

No Longer Use Threshold

Maintenance

- Asset management
  - Access and authorization
  - Physical Access
- Scheduled maintenance
- On demand maintenance
- Parts sourcing and inventory
- Operating and service manuals, instructions for use, technical bulletins
- User training

- Specialized management tools
  - CMMS = Work Orders = Uptime requirements
  - CMDB = Tickets = SLA response times
- Correlation is essential

RACI

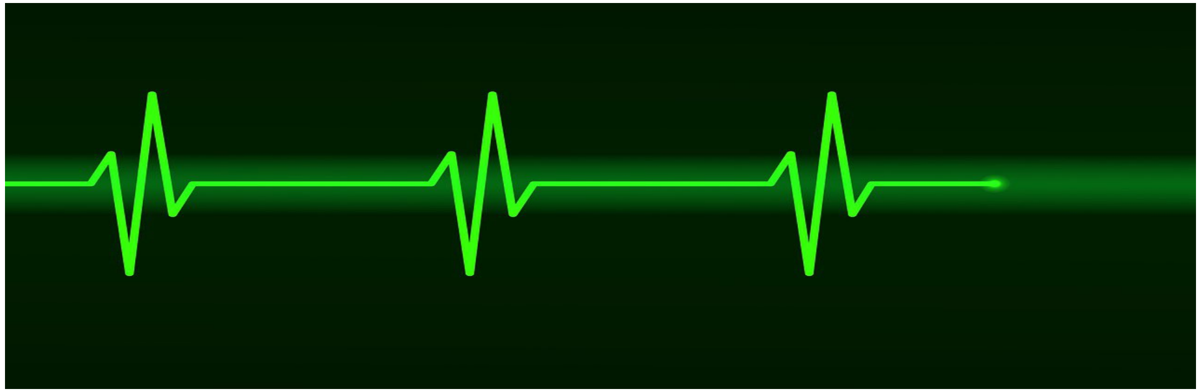
Tasks	HDO Technology	HDO Clinical	MDM Product	MDM Support
Secure Configuration	RA	I	C	
OS Patching	C	I	A	R
Clinical Application Update	I	A	C	R
Interface Updates	R	A	C	
Remote Access Control	RA	C		C

- Responsibility Assignment Matrix
  - Responsible – the doer
  - Accountable - the decider
  - Consulted – the provider
  - Informed – kept abreast
- Integral with
  - Service strategy
  - Response plan

Monitoring

- Scheduled maintenance compliance
- Changes in failure rates
- Changes in failure types
- Service logs
- Changes in cost of service
- Quality issue investigation
- Lost/missing assets
- Location

- Vulnerability monitoring
- Comms traffic patterns
- Comms traffic anomalies
- Event logs
- Last activity



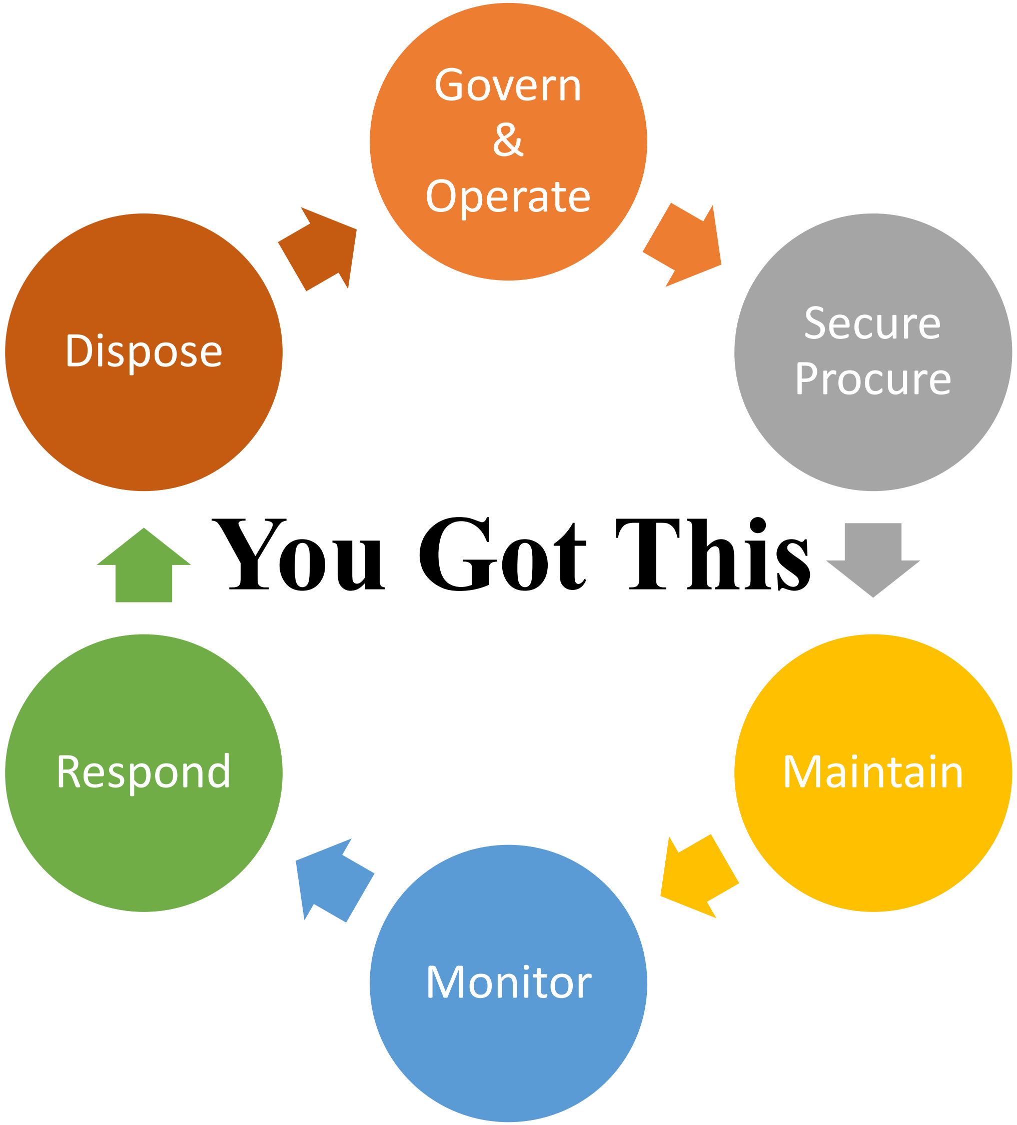
Response

- On demand repairs
- Clinician assistance
- Equipment check
- Planned maintenance
- Help desk
- RTO
  - Recovery Time Objective
  - Return to Operations
- RPO
  - Recovery Point Objective

- Risk Assessment is key but which one?
  - Organizational Impact
    - Elements
      - Patient, staff safety
      - PHI, Big PHI
      - Operational Interruption
      - Revenue slash
      - Reputation
    - Prioritizes everything

Disposal

- Drivers
  - Final Failure
  - Planned replacement
  - End of Support
  - Repurpose
- Requirements
  - Remove organizational risks
    - PHI, credentials, configuration, etc.
- Plan disposal during onboarding
  - Push PHI to the data center
  - Ghosted hard drive



- Understand the risk
- Consistent prioritization
- Business owns risk
- Team sport

Questions?