Medical Device Cybersecurity

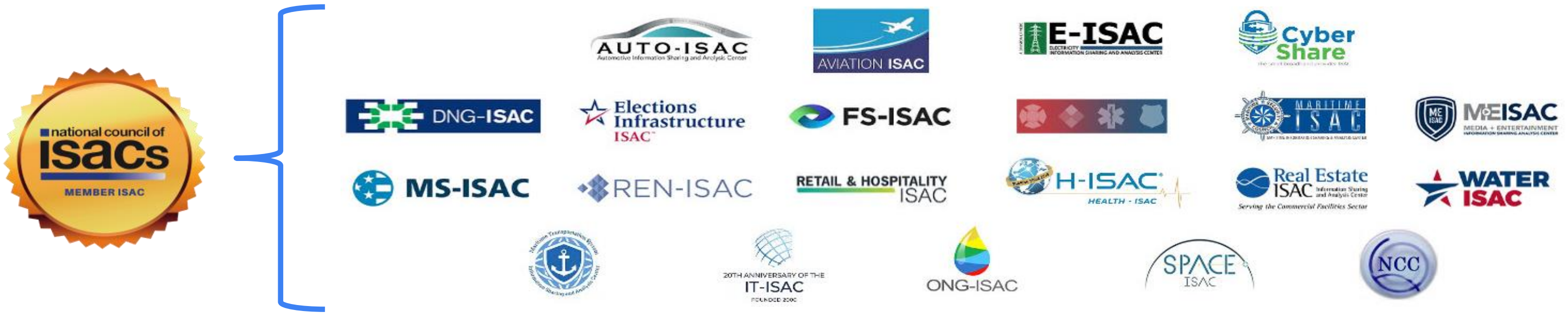
Phil Englert

VP Medical Device Security
Health-ISAC

MDEXPO
Las Vegas • April 7-9, 2024

What is an ISAC?

- ISAC is short for “Information Sharing and Analysis Center”
- ISACs empower **sharing and collaboration** in critical infrastructure communities to prevent, detect, and respond to cybersecurity and physical security events
- ISACs collect, analyze, and disseminate actionable **threat information** to their members and provide them with **tools** to mitigate risks and enhance resiliency



Membership Overview

Health-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating, and sharing vital physical and cyber threat intelligence and best practices.

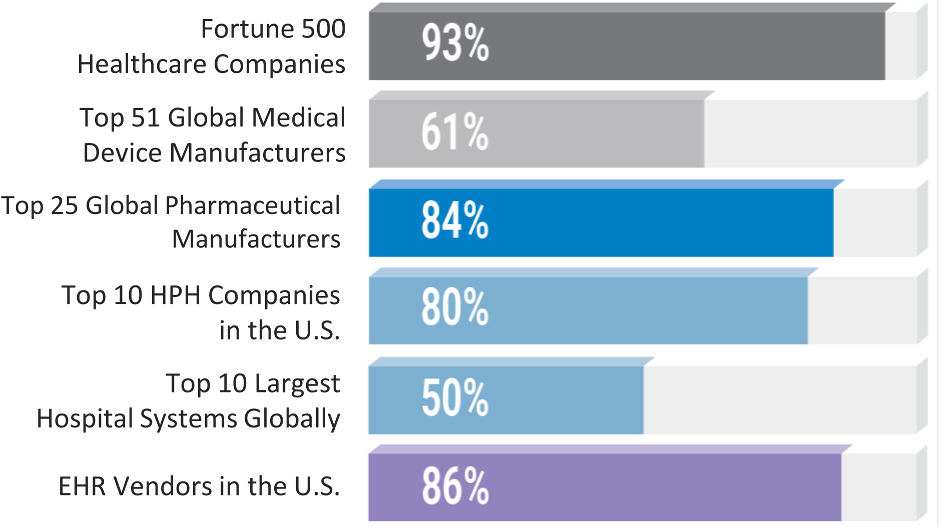
About Health-ISAC

- Community of 8,000+ Global Security Analysts, built on **trust** and **anonymity**
- Members must be in the health sector and interested in providing value to the overall Health-ISAC eco-system by listening, sharing, and/or contributing
- Ideal organizations for membership:

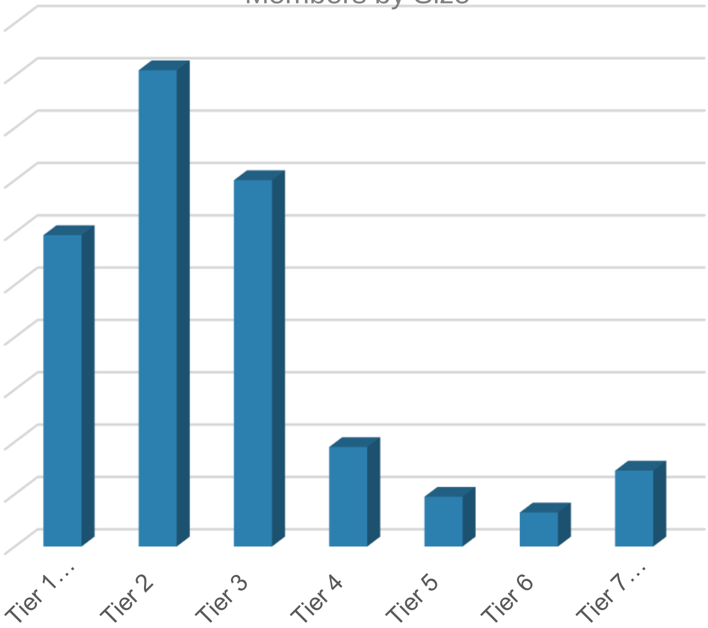
Healthcare Providers
Insurance (Payers)
Academic Medical Schools
Medical Device Manufacturers (MDM)
Electronic Medical Records (EMR)
Group Purchasing Organizations (GPO)
Pharmaceutical
Pharmacies
Telehealth
Laboratories
Radiological Centers
Revenue Cycle Management
Healthcare Supply Chain
Mortuaries
R&D Centers
Hospice
Clearing Houses
Genomics

Member Demographics

Health-ISAC
Members include:



Health-ISAC
Members by Size



Board of Directors

MERCK

abbvie

PREMERA BLUE CROSS

GUTHRIE

AMGEN

Humana

Pfizer

Rady Children's

PHILIPS

Takeda

HCA Hospital Corporation of America

Mount Sinai

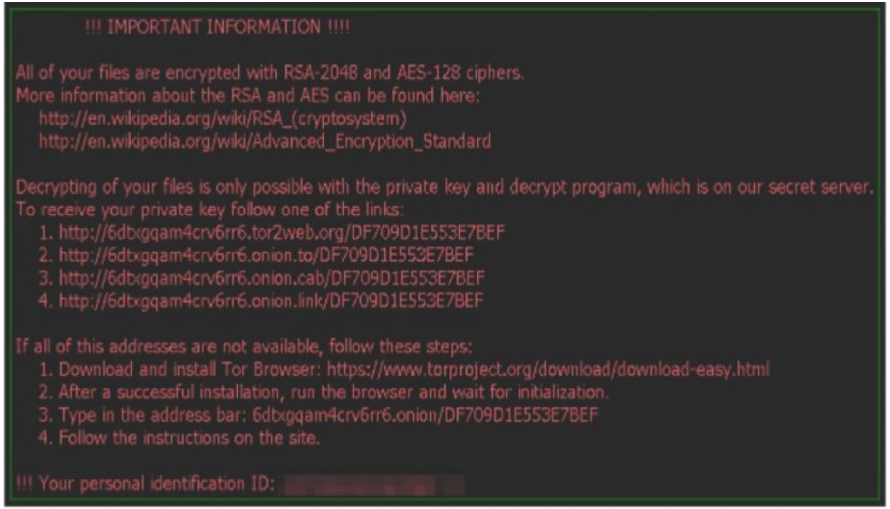
DANAHER

MCKESSON

ChristianaCare™

Healthcare is under attack

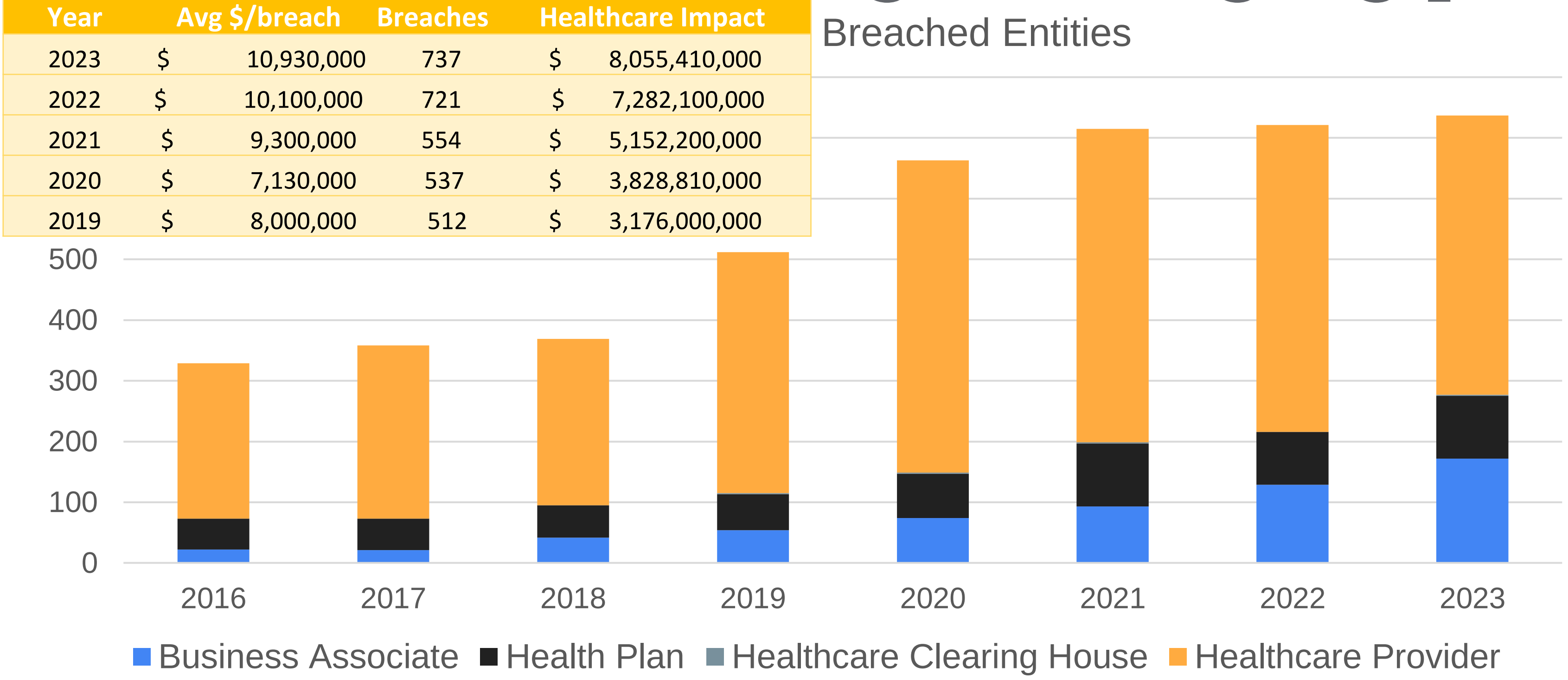
- Hollywood Presbyterian Medical Center
- 434-bed Level II trauma center serving a multicultural urban LA community
- Feb. 5, 2016 – staff reported inability to access records
- Internal emergency declared
- Record access/sharing not possible
- Patients diverted
- FBI & local Law enforcement called in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



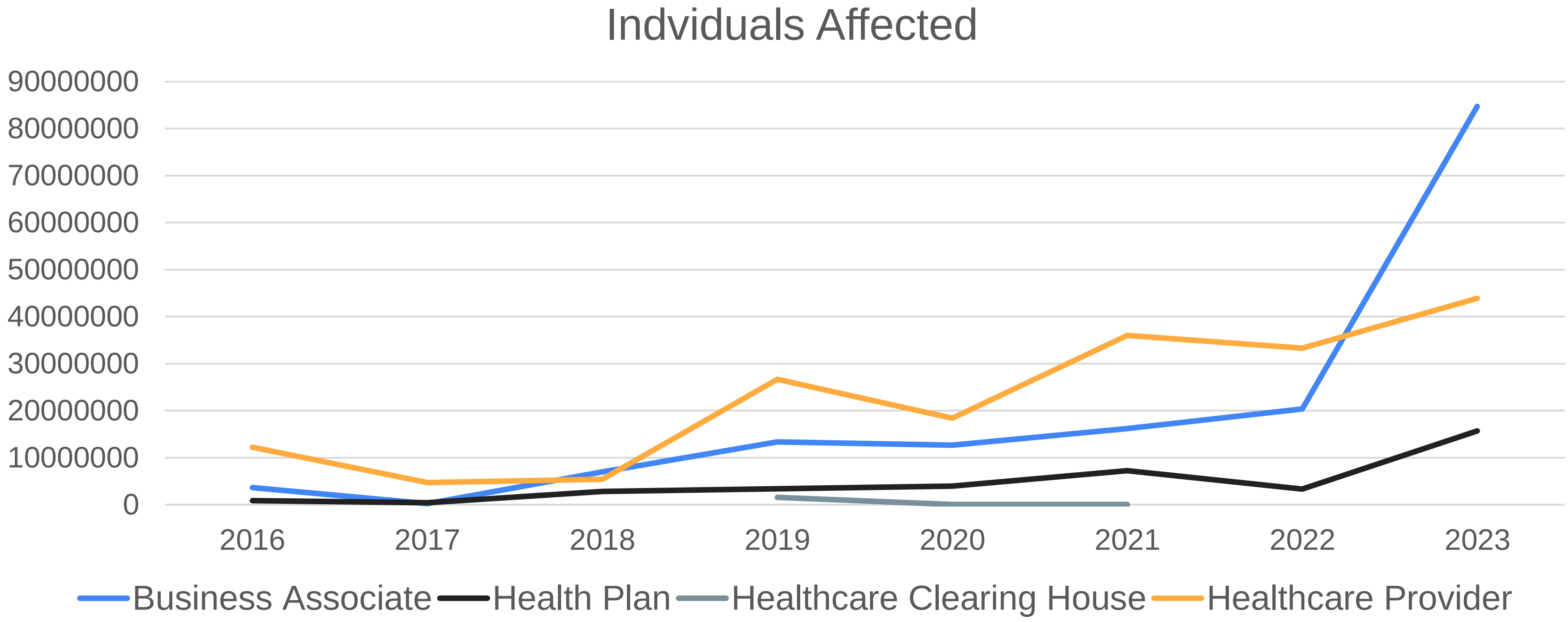
```
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org/DF709D1E553E7BEF
    2. http://6dtxgqam4crv6rr6.onion.to/DF709D1E553E7BEF
    3. http://6dtxgqam4crv6rr6.onion.cab/DF709D1E553E7BEF
    4. http://6dtxgqam4crv6rr6.onion.link/DF709D1E553E7BEF

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/DF709D1E553E7BEF
    4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]
```

Breach count by entity type

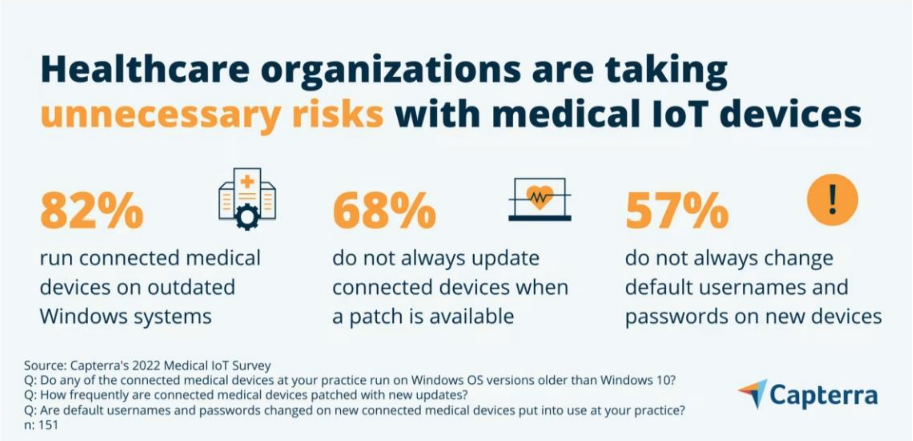
Year	Avg $/breach	Breaches	Healthcare Impact
2023	$ 10,930,000	737	$ 8,055,410,000
2022	$ 10,100,000	721	$ 7,282,100,000
2021	$ 9,300,000	554	$ 5,152,200,000
2020	$ 7,130,000	537	$ 3,828,810,000
2019	$ 8,000,000	512	$ 3,176,000,000



Individual records by entity type



Survey Says!



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

Capterra

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

- 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.

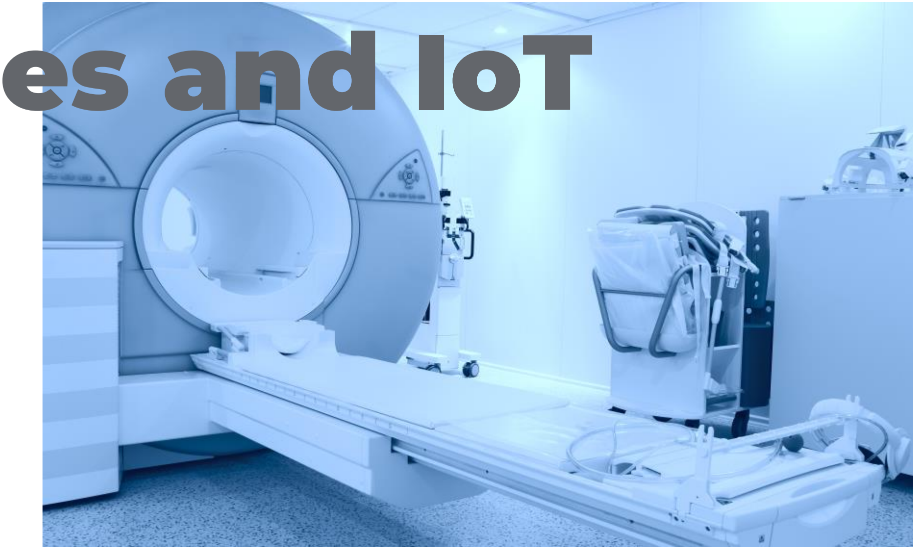
https://www.capterra.com/resources/medical-internet-of-things-iot-security/

A woman dies during a cyberattack 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



Medical Modalities

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

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

Security incidents will grow

2019: Implanted defibrillators telemetry protocol flaw

Some implanted defibrillators were found to contain vulnerabilities that would allow them to be 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

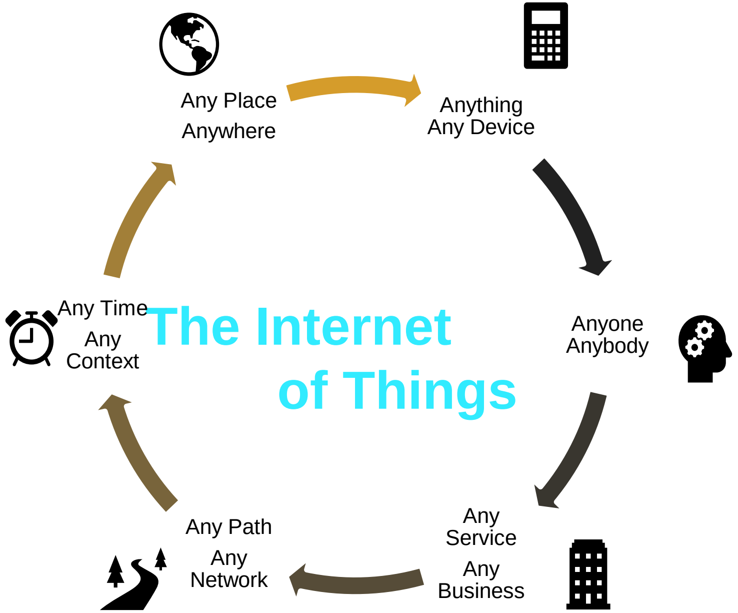
PACS (picture archiving and communication system) are used for picture archiving and communication system. Security researchers found several vulnerabilities both in commercial and open-source PACS.

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 to be so serious that they could cause severe injury or death, even just by plugging a phone into the USB port.

Internet of things

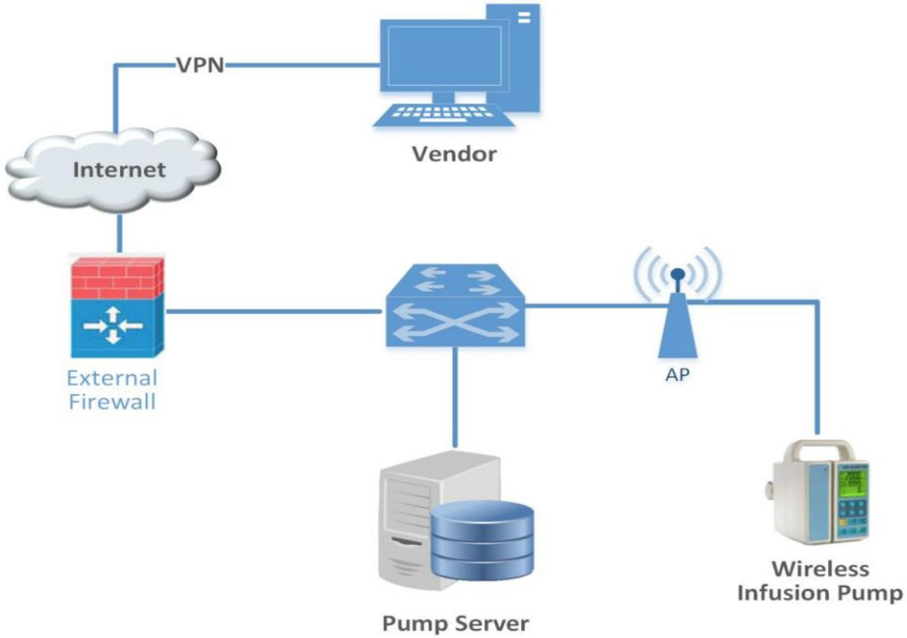
- Global IoT spending is expected to reach $1t in 2023
- 7b IoT devices
  - 3x to 24b by 2030
- US medical device manufacturing revenue $50b in 2023
- 3.4% growth rate
- US healthcare expenditure
  - $4.3t in 2021 ($12,914/person)
- 16.8% of gross domestic product (GDP) in 2019



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.

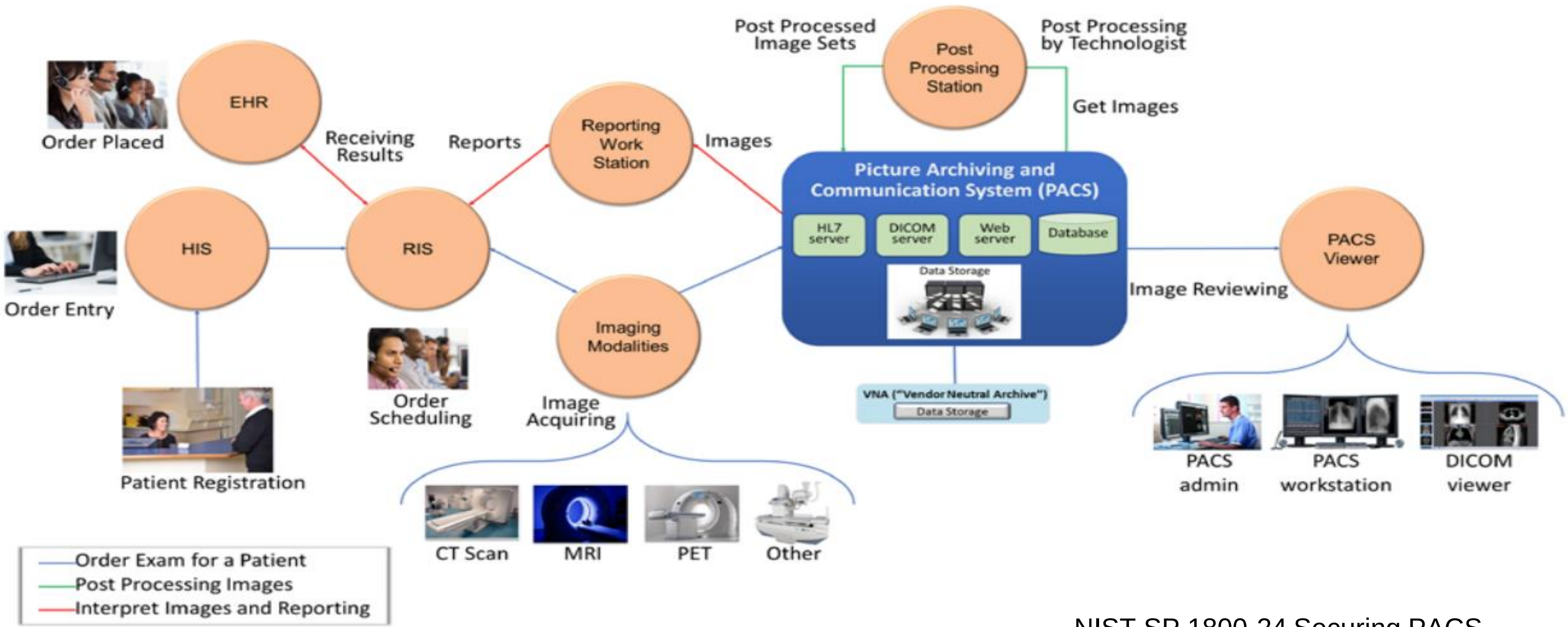
Basic infusion pump management system

Figure 5-1 Basic System



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

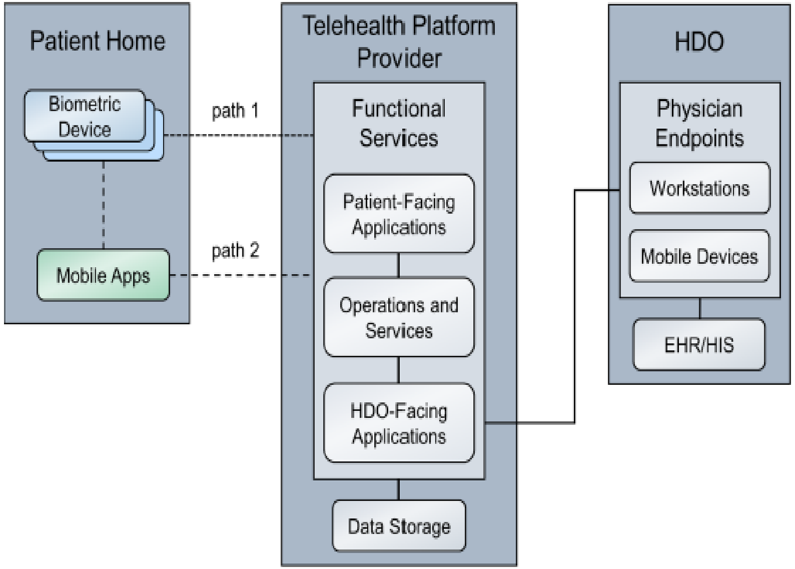
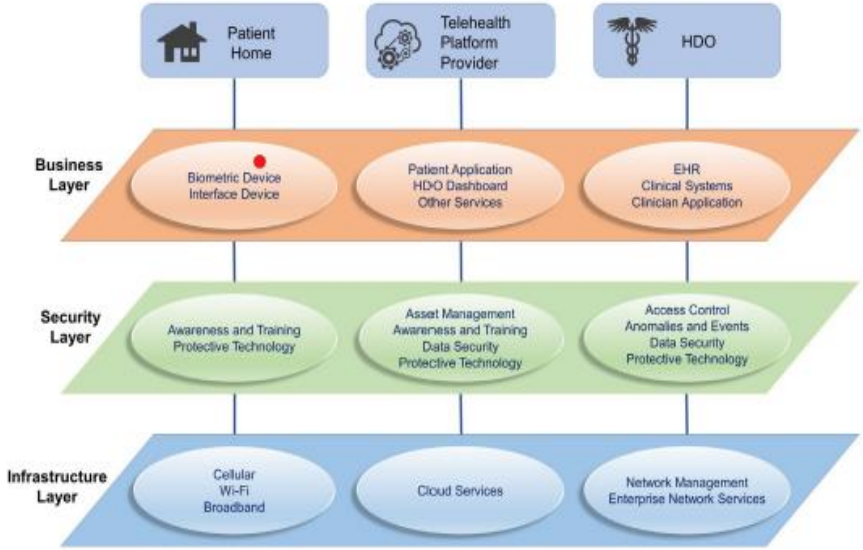


Figure 4-2 Architecture Layers


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

Healthcare matrix

- 6,400 acute care hospitals
- Urban teaching or trauma
- Suburban & Community
- Rural and critical access
- Diagnostic and surgery centers
- Clinics, wellness, and pharmacy
- Physician practices

- 100+ hospital system
- 380,000+ medical devices
- Approximately 100k connectable
- 1,200 makes and models
- 500+ manufacturers
- ~20 manufacturers account for 80% of device count

- FDA >560 product codes for software-enabled medical devices

FDA Update

1. Granted Statutory Authority over Cybersecurity
    1. Section 3305 Omnibus Appropriations Bill 2022
    2. Ensuring cybersecurity of medical devices
    3. Modifies SEC. 524B. of FDA&C
2. Effective March 29, 2023, for new submissions

Alignment

Omnibus 2023	FDA Premarket Guidance
Secure by Design: design, develop, and maintain processes and procedures	Secure Product Development Framework (SPDF) Cybersecurity is patient safety
a plan to monitor, identify, and address in a reasonable time, postmarket cybersecurity vulnerabilities and exploits	TPLC: identify, assess, and mitigate cybersecurity vulnerabilities…**throughout the** supported device **lifecycle**
make available postmarket updates and patches to the device	Security Objective: Secure and timely updatability and patchability
Software bill of materials, including commercial, open-source, and off-the-shelf software components	SBOM on a continuous basis in a machine-readable format
Demonstrate reasonable assurance of the safety and effectiveness of devices, a reasonable assurance of the cybersecurity	demonstrate the effectiveness of the controls in a proper security context to provide a reasonable assurance of safety and effectiveness
Third party data transparency	Cybersecurity transparency

FDA Premarket Guidance highlights

1. Quality System Regulations
2. Cybersecurity is Patient Safety
3. Secure Product Development Framework
4. Security Objectives drive Security Requirements and Security Controls
5. Cybersecurity Transparency & Labelling
6. Security Risk Management
7. Threat Modelling, Security Architecture, & Cybersecurity Testing

Quality System Regulations (QSR) 21 CFR Part 820

- **Secure Product Development Framework (SPDF)** a set of processes that help reduce the number and severity of vulnerabilities

1. Security Objectives:
   a. Authenticity, which includes integrity;
   b. Authorization;
   c. Availability;
   d. Confidentiality;
   e. Secure and timely updatability and patchability.

2. Security requirements depend on:
   a. the device's intended use and indications for use;
   b. the presence and functionality of its electronic data interfaces;
   c. its intended and actual environment of use;
   d. the type of cybersecurity vulnerabilities present;
   e. the exploitability of the vulnerabilities; and
   f. the risk of patient harm due to vulnerability exploitation.

Hospital ransomware attack allegedly led to infants 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, C-section with wrapped umbilical cord
- 1st confirmed death pending court outcome

•CVE-2018-8453 - high-severity (7.8/10) privilege escalation in Windows 7 - 10 and Windows Server 2008 - 2016
•CVE-2019-1069 - high-severity (7.8/10) privilege escalation in Windows 10, Windows Server 2016, & 2019
•Patch systems against CVE-2018-8453 and CVE-2019-1069

Complex Lifecycle management

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

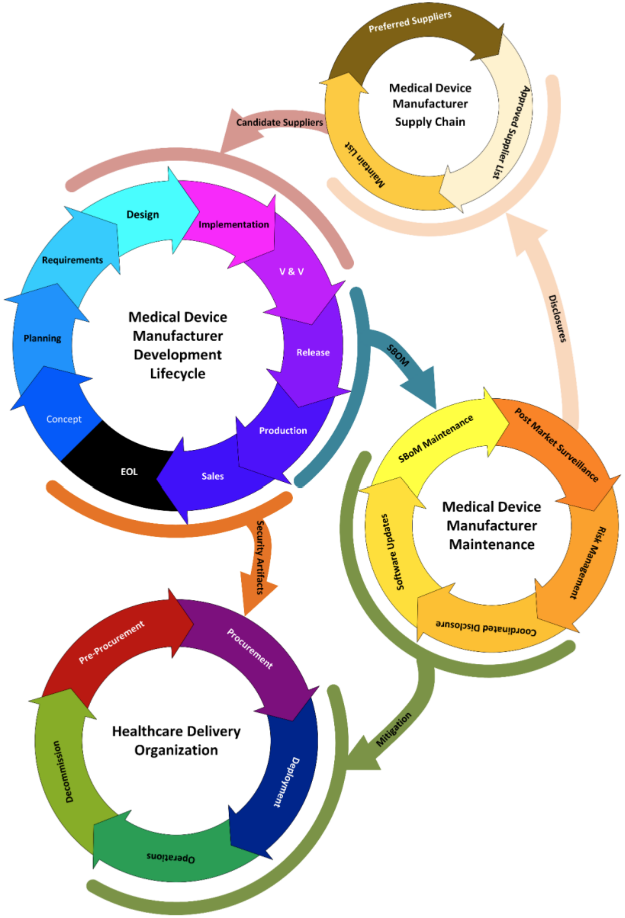
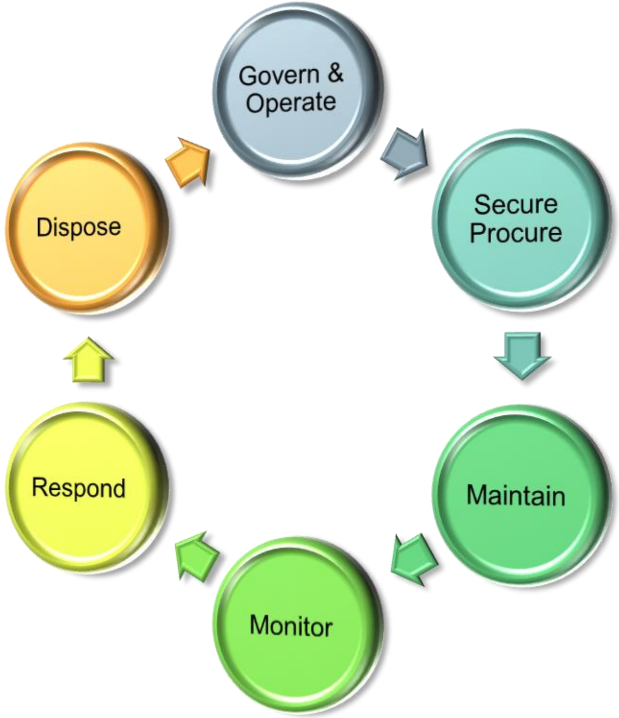


Figure 1: Main Areas and Phases of Lifecycle Management

Medical Device Cybersecurity Program

1. Governance & Operating Model
2. Secure Procurement
3. Maintenance
4. Monitoring
5. Response
6. Disposal



CCTVnerds

2,399 followers

4d •

+ Follow

When the security budget is low...

You know what to do

- HTM job #1 is maintenance operations
- Cyber is a failure mode
- Anticipate and respond

Governance & Operating Model

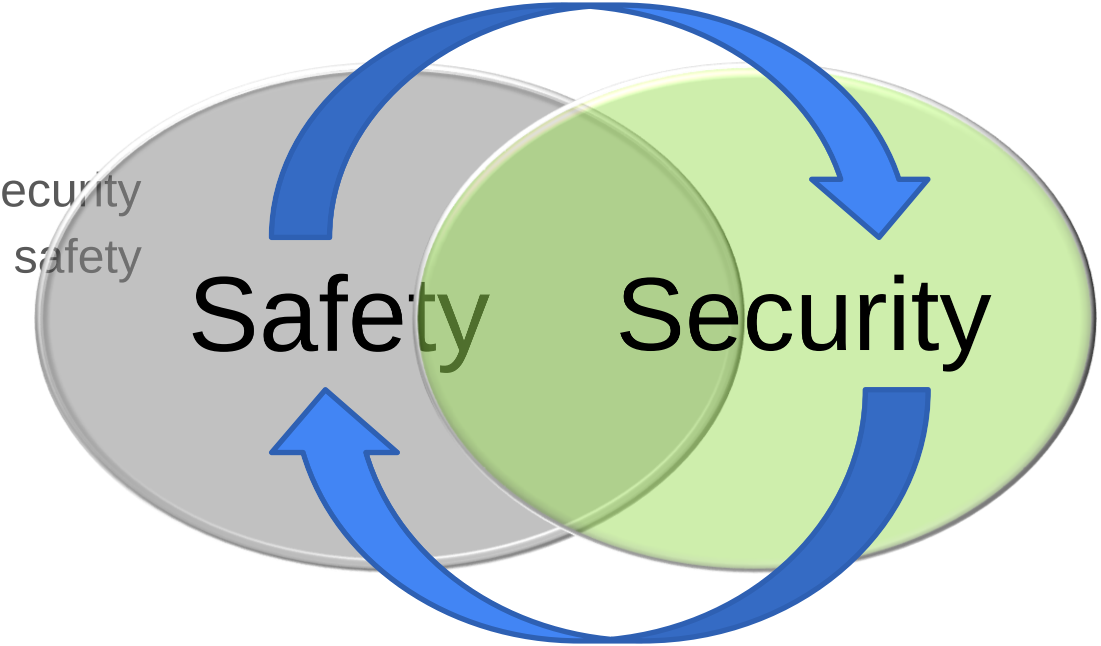
- Governance
  - Who makes what decisions
    - Environment of Care
      - Regulatory requirements
      - Risk Management
      - Patient Safety
    - Performance Improvement Plans
    - Spending authority
    - Data Protection
    - Staff Management
    - Education & Training

- Operating Model
  - Medical Equipment Management Plan
    - 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
- Cyber not just failure – **intent**

- **Business owner's decision**



Asset management

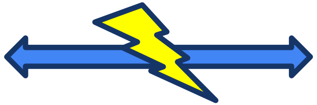
HTM

- Install base alignment
- Incoming Inspection
- Asset ID, RFID
- Make, model, version
- Passive scanning

IT

- Standards compliance
- Risk assessment
- IP address, MAC address
- OS & patch level, components
- Vulnerability scanning

- Uptime requirements



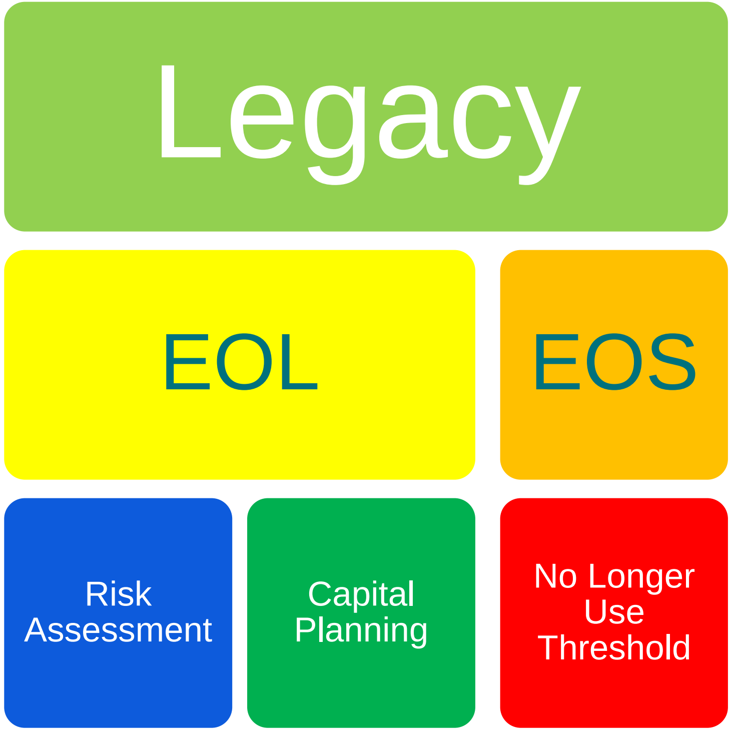
- SLA response times

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 safe

Legacy equipment

- AHA Useful life is often 7-12 years
- OS is out of support
- Manufacturer no longer supports
- Bailing wire and bubblegum
- Clinically useful i.e., still works fine
- 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
  - X CMMS ID = Y CMDB ID

RACI

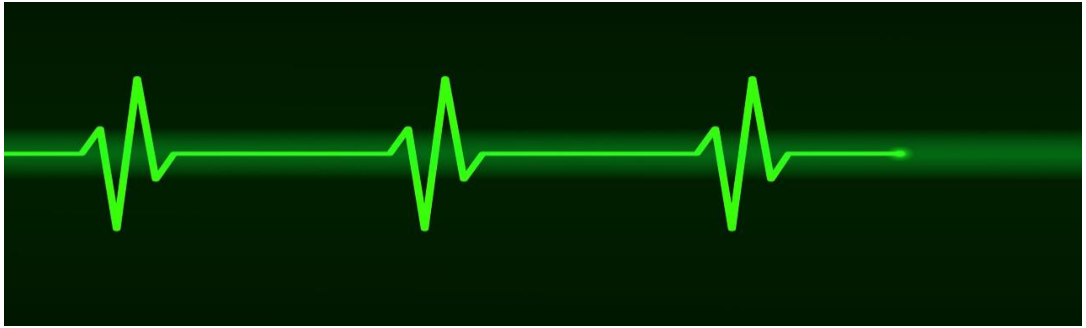
- Responsibility Assignment Matrix
  - Responsible – the doer
  - Accountable - the decider
  - Consulted – the advisor
  - Informed – kept abreast
- Integral with
  - Service strategy
  - Response plan

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

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
- RPO
    - Recovery Point Objective
- **Return to Operations**

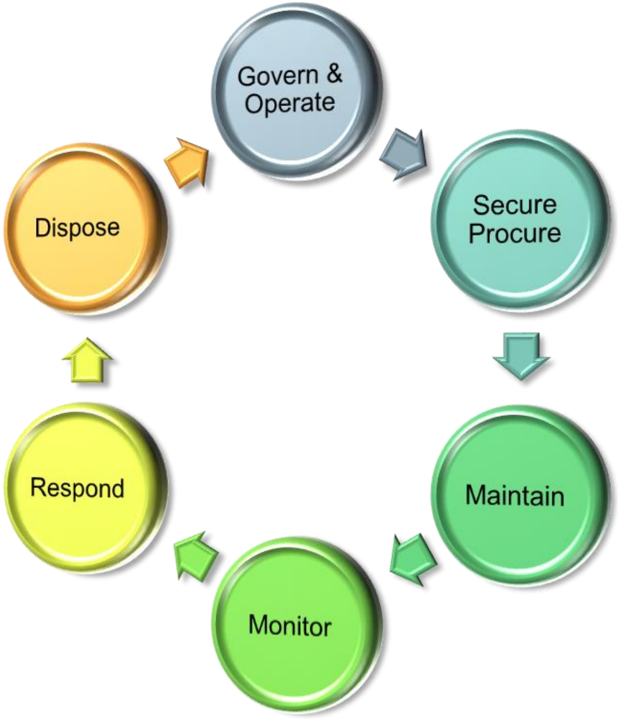
Risk Assessment is the key

- Organizational Impact
    - Elements
        - Patient, staff safety
        - PHI, Big PHI
        - Operational Interruption
        - Revenue
        - 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
  - Clone a hard drive

You got this !



- Key Take Aways

1. Understand the risk
2. Consistent prioritization
3. Business owns risk
4. Team sport

- **Do One Thing** – Go to a department leader and ask what equipment, if lost for 4-5 days, would cause them to shut down services and help devise a plan to prevent that

(ISC)^{2}®

- International Information System Security Certification Consortium
- Certified in Cybersecurity – CC
- https://www.isc2.org/certified-in-cybersecurity?filter=featured&searchRoot=A82B5ABE5FF04271998AE8A4B5D7DEFD

Phil Englert

VP Medical Device Security

- **Industry roots:**
- *Field Service Engineer, Clinical Diagnostics*
- *Biomedical Manager, 14 hospitals*
- *System Director, Technology Operations @ Catholic Health Initiatives (23 years)*
- Vice President of Health Systems @ Medical Device Innovation Security and Safety Consortium (MDISS)
- Global Leader for Medical Device Cybersecurity @ Deloitte

- (e) penglert@h-isac.org
- (m) +1 859.393.7140

Sector Leadership:

Cybersecurity Infrastructure and Security Agency (CISA) Vulnerability Communications TG

Health-ISAC SBOM Proof of Concept WG

Health Sector Coordinating Council TG-1D - Supply Chain / Third Party Cyber Risk Management / Model Contract Language for MedTech Cybersecurity / CWG OT Manufacturing / CWG Measurement TG

National Telecommunications and Information Administration (NTIA) SBOM, Healthcare; Framing, and Proof of Concept workgroups

Underwriters Laboratories, Standards Technical Panel; STP 2900-1, STP 2900-2-1

MITA MDS2, Manufacturers Disclosure Statement for Medical Device Security, 2019 revision

US Board of Examiners for Certification in Clinical Engineering

This Photo by Unknown Author is licensed under CC BY