HIPAA Summit XXVII

Panel Discussion:
Securing Medical Devices and the IoT in Healthcare

March 28, 2018

https://hipaasummit.com/agenda-day-2/

Today's Panelists

MODERATOR

Bob Chaput MA, CISSP, HCISPP, CRISC, CIPP/US

CEO

Clearwater Compliance

Sheetal Sood, CHC, CIPP, CISSP, CISA, CRISC, GSEC, MCSE

Senior Executive Compliance Officer,

Information Governance

NYC Health + Hospitals

Aftin Ross, PhD

Senior Project Manager

Senior Science Health Advisor

Food and Drug Administration

Sue Wang

Technical Lead of the Healthcare Sector Team in the National Cybersecurity FFRDC, National Cybersecurity Center of Excellence (NCCoE) at NIST

Dana-Megan Rossi, JD

BU Product Security Officer,

Technology Solutions

Becton Dickinson

First Healthcare Risk Manager

"First, Do No Harm."

-Hippocrates, 4th Century, B.C.E.
-OR

-Auguste François Chomel (1788–1858) Parisian pathologist and clinician
-OR

-???

Digitization in Healthcare is Great … AND Now, We Can Create Harm from New Threat Sources

Key Themes

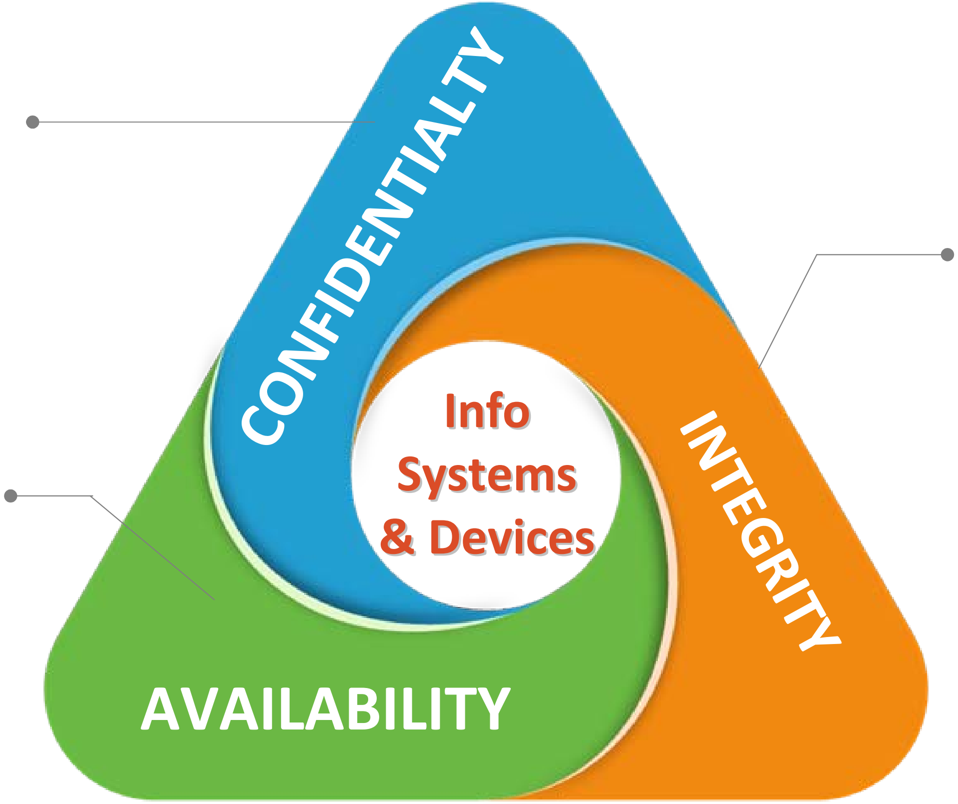
1. We must connect the dots between cyber risk and patient safety
2. We need to look beyond traditional IT assets to biomedical devices and the Internet of Things (IoT)
3. Risk analysis and risk management should be applied to all assets
4. And, to be successful, industry collaboration such as that which produced the Wireless Infusion Pump Practice Guide must continue

The Risk Problem We're Trying to Solve

What if Sensitive Information is shared?

What if Sensitive Information is not complete, up-to-date and accurate?

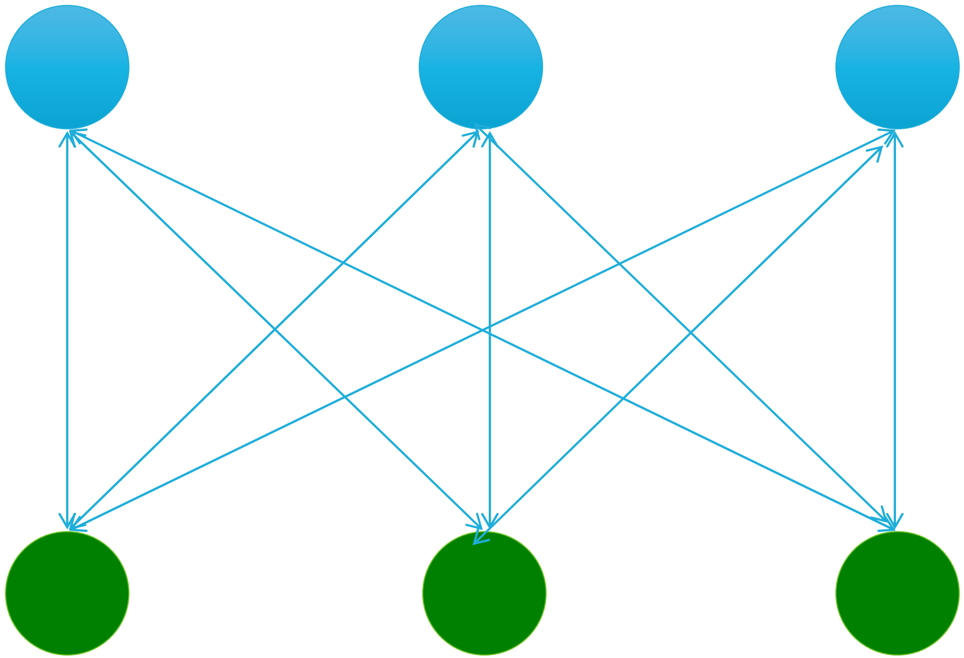
What if Sensitive Information, Systems or Devices are not there when it is needed?



Don't Compromise C-I-A!

Single Biggest Issue: Risk Identification

Connect the Dots Between Cyber Risks and Patient Safety



Confidentiality

Integrity

Availability

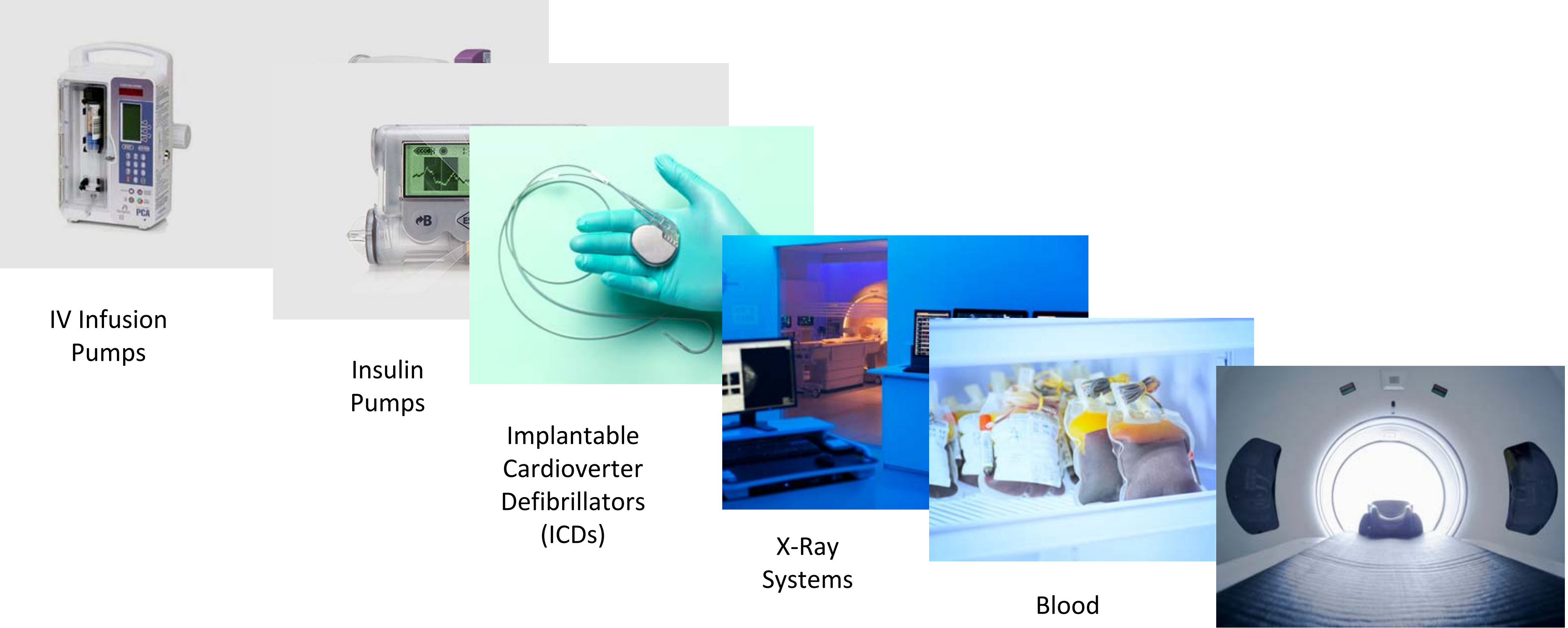
Quality and Safe Care

Access to Care

Timely Care

Patient Information AND Patient Health

Need to Look Beyond Traditional IT Assets



IV Infusion Pumps

Insulin Pumps

Implantable Cardioverter Defibrillators (ICDs)

X-Ray Systems

Blood Refrigeration Units

CT Scans

Cyber Attacks on CT Scan Devices

Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices

Configuration File Corruption

Mechanical Disruption of Device's Motors

Ransomware DoS

Modification of Image Results

Unauthorized Access of Images

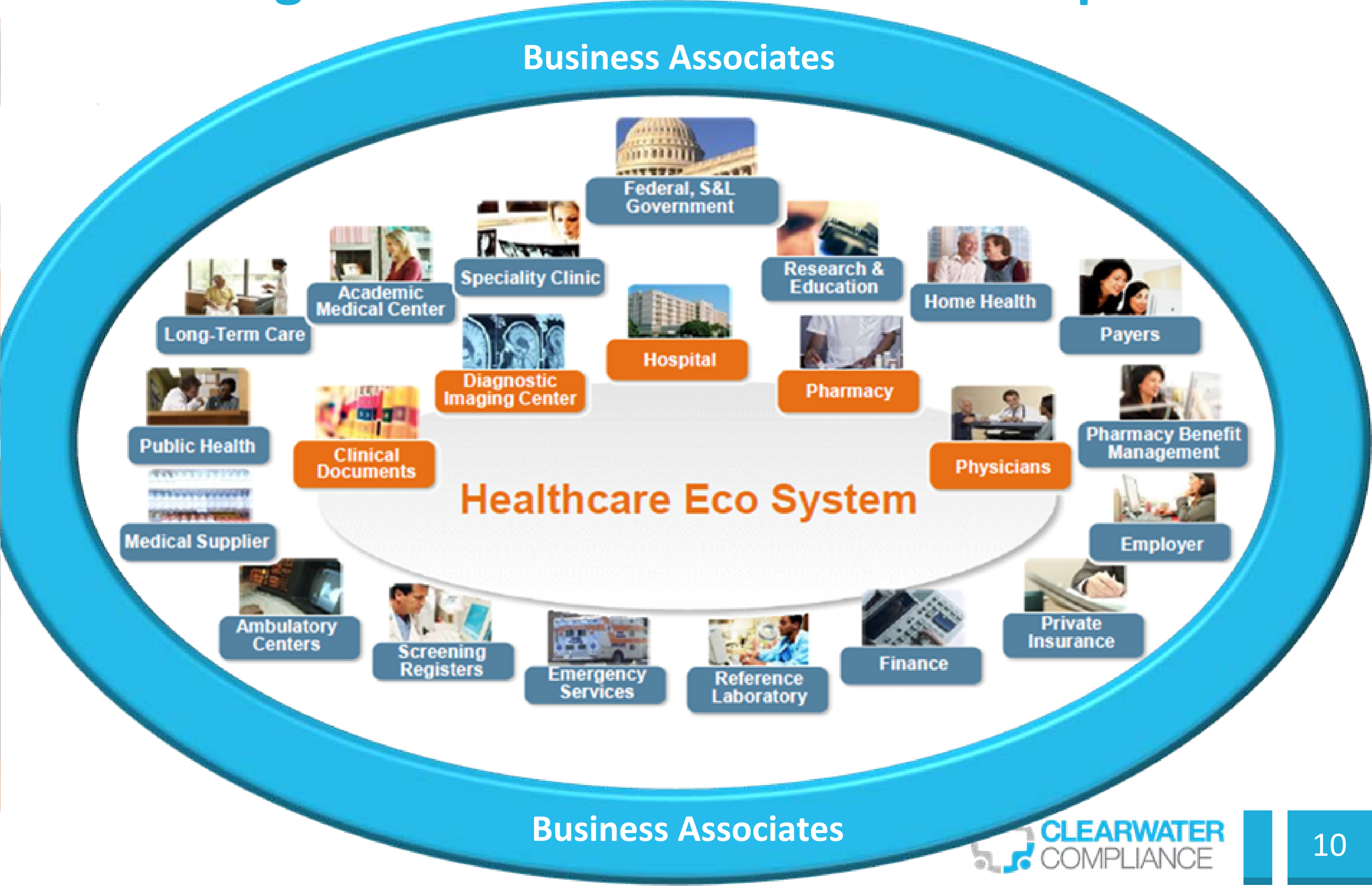
https://arxiv.org/abs/1801.05583

Information Assets & OCR-Quality Risk Analysis

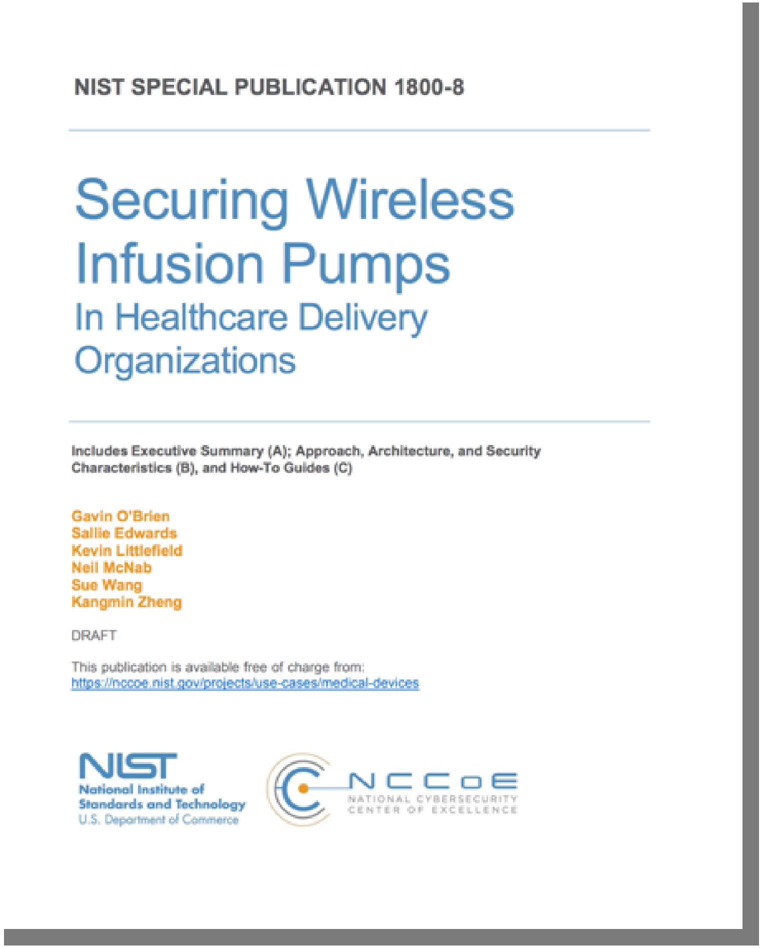
Scope of the Analysis: *The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of* ***all e-PHI*** *that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).) This includes* ***e-PHI in all forms*** *of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus,* ***an organization's risk analysis should take into account all of its e-PHI****, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.*

"Guidance on Risk Analysis Requirements under the HIPAA Security Rule"

Information Risk Management Must Become a Team Sport



Include Biomedical Devices in Risk Analyses



NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps

In Healthcare Delivery Organizations

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C)

Gavin O'Brien
Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use-cases/medical-devices

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- NIST is increasing activity and work products
- First Practice Guide published May 2017
- Government and industry collaboration
- NIST-based risk assessment performed

B|BRAUN Baxter BD CISCO CLEARWATER COMPLIANCE digicert Hospira intercede

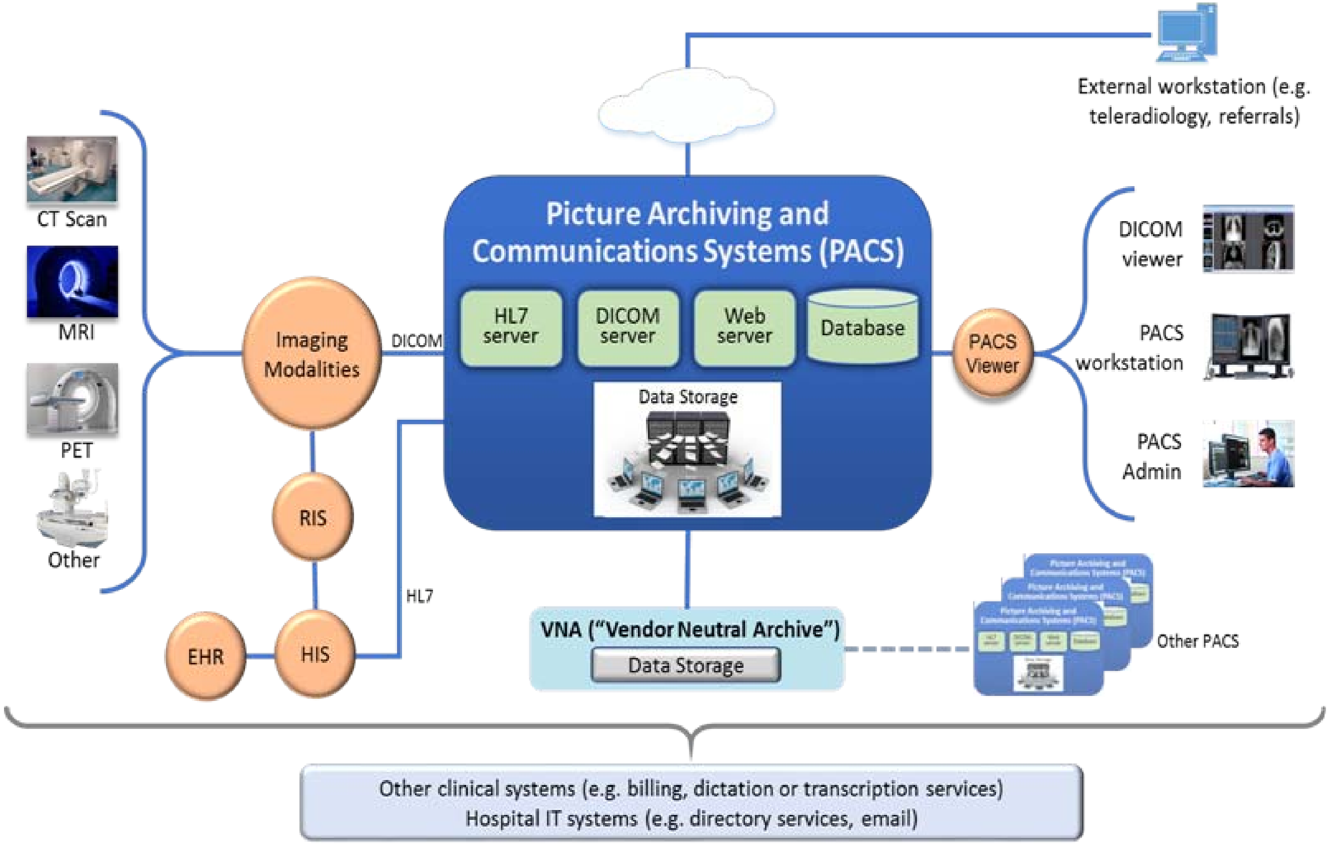
MDISS PFP CYBERSECURITY RAMPARTS smiths medical bringing technology to life Symantec TD

https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Securing Picture Archiving and Communication System (PACS)

Picture Archiving and Communication System (PACS)


External workstation (e.g. teleradiology, referrals)
CT Scan
MRI
PET
Other
Imaging Modalities
DICOM
RIS
HL7
EHR
HIS
Picture Archiving and Communications Systems (PACS)
HL7 server
DICOM server
Web server
Database
Data Storage
PACS Viewer
DICOM viewer
PACS workstation
PACS Admin
VNA ("Vendor Neutral Archive")
Data Storage
Other PACS
Other clinical systems (e.g. billing, dictation or transcription services)
Hospital IT systems (e.g. directory services, email)

Final Project Description: https://nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-pacs-project-description-final.pdf

Tools – Tips For Identifying Information Assets

- Medical devices
  - Sitter cameras, infusion pumps, imaging modalities, laboratory devices, vital signs monitoring
  - Scan for medical devices communicating on the network
    - www.medigate.io
  - Leverage the Manufacturer Disclosure Statement for Medical Device Security (MDS2) for the discovered devices

- Internet of Things (IoT)
  - Thermostats, DVD players, lighting systems, appliances, HVAC, IP Video Cameras
  - Scan for IoT devices connected to the network
    - https://nmap.org/
    - fingerbank.org

IoT Asset Discovery and Identification

Step 1: Discovery

https://nmap.org/

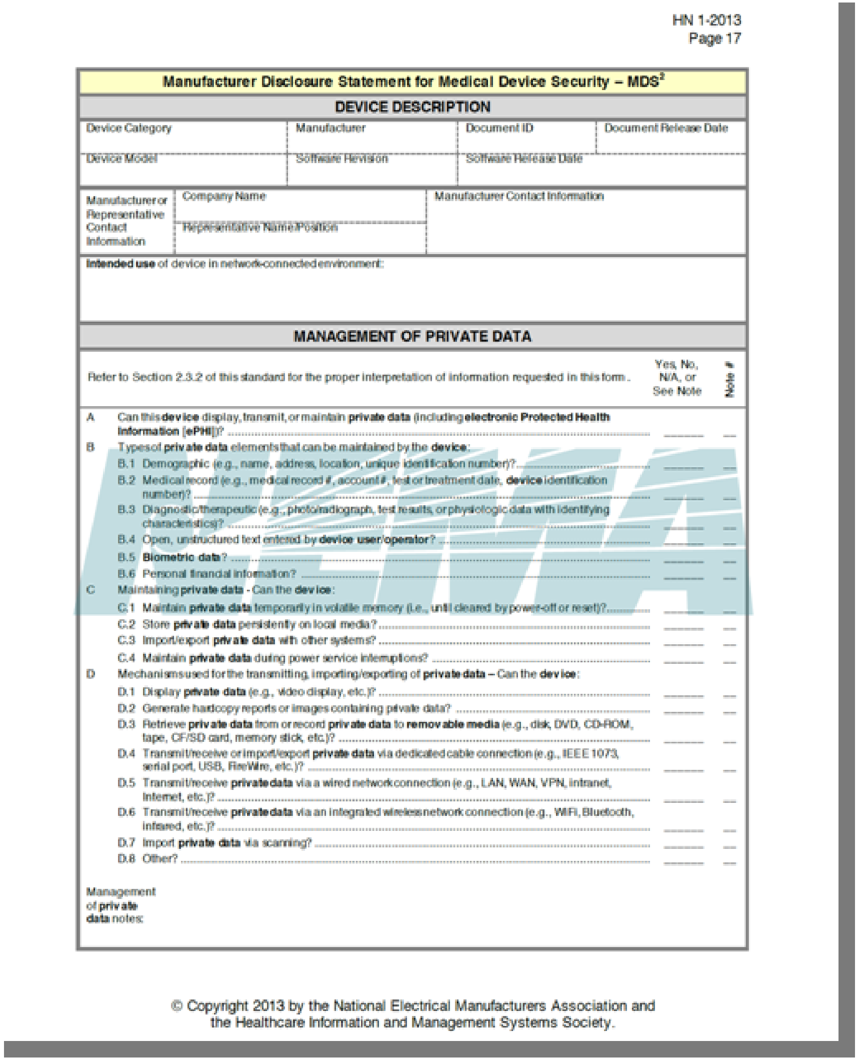
Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. https://nmap.org/

Step 2: Identify and Digital Fingerprint

https://fingerbank.org/

Fingerbank accurately determines what kind of device is connected on a network based on its MAC address, its DHCP fingerprint, its User-Agent, its TCP signatures, its network behavior and more. Fingerbank can accurately identify Internet of Things (IoT) devices, medical devices, industrial and robotics equipment and more.

Manufacturer Disclosure Statement for Medical Device Security (MDS²)



HN 1-2013
Page 17

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	
Manufacturer or Representative Contact Information	Company Name Representative Name/Position	Manufacturer Contact Information	

Intended use of device in network-connected environment:

MANAGEMENT OF PRIVATE DATA

		Yes, No, N/A, or See Note	Note #
	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	____	__
B	Types of **private data** elements that can be maintained by the **device**:		
	B.1 Demographic (e.g., name, address, location, unique identification number)?	____	__
	B.2 Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	____	__
	B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	____	__
	B.4 Open, unstructured text entered by **device user/operator**?	____	__
	B.5 **Biometric data**?	____	__
	B.6 Personal financial information?	____	__
C	Maintaining **private data** - Can the **device**:		
	C.1 Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	____	__
	C.2 Store **private data** persistently on local media?	____	__
	C.3 Import/export **private data** with other systems?	____	__
	C.4 Maintain **private data** during power service interruptions?	____	__
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1 Display **private data** (e.g., video display, etc.)?	____	__
	D.2 Generate hardcopy reports or images containing private data?	____	__
	D.3 Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	____	__
	D.4 Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	____	__
	D.5 Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	____	__
	D.6 Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	____	__
	D.7 Import **private data** via scanning?	____	__
	D.8 Other?	____	__

Management of **private data** notes:

- Originally developed by HIMSS and the American College of Clinical Engineering (ACCE), and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association (NEMA)
- The MDS² provides medical device manufacturers with a means for disclosing issues to healthcare providers
- The MDS² form can be used as a tool in an organization's risk assessment process
- Provides a comprehensive set of medical device security questions developed through broad stakeholder participation and medical device vendor buy-in
- Allows for easy comparison of security features across different devices and different manufacturers
- Facilitates the review of the large large volume of security-related information supplied by the manufacturers

http://www.himss.org/resourcelibrary/MDS2

Resources

1. AAMI TIR57, Principles for medical device security – risk management
2. Guidance on Risk Analysis Requirements under the HIPAA Security Rule
3. IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
4. ISO 14971 Medical devices — Application of risk management to medical devices
5. FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance
6. FDA Postmarket Management of Cybersecurity in Medical Devices
7. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)*
8. *THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY*
9. NIST SP1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations - DRAFT
10. NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessments
11. NIST SP 800-37 Rev1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
12. NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View