ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

2023 CCE Written Exam Review Webinar Series

August 9, 2023, through October 11, 2023

Session #8 IT/Telecommunications (IT Part 2)

September 27, 2023

Faculty: Ted Cohen, MS, CCE, FACCE

tedcohen@pacbell.net

About the host/moderator

Kajal Madhusudan

Kajal Madhusudan is a Clinical Engineer at Children’s Hospital of Eastern Ontario (CHEO). She earned her Masters degree in Biomedical Engineering with a concentration in Clinical Engineering from the University of Ottawa.

Kajal holds the designation of Engineering Intern (EIT) with Professional Engineers Ontario (PEO), signifying her progress towards becoming a licensed Professional Engineer. Kajal also holds the position of Computerized Maintenance Management System (CMMS) Administrator at CHEO. In this role, she has shown her ability to efficiently manage and optimize the hospital's maintenance database, ensuring smooth operations and patient care.

Logistics

❖**All attendees have their microphones muted during the presentation.**

❖**Questions to the panelists must be submitted via the "Q&A" feature in Zoom at any time. They will be addressed at the Q&A portion.**

❖**If there is any urgent issue, please use the "chat" feature to communicate with the panelists/host.**

❖**Please remember to complete the webinar evaluation after attending. A link will be provided at the end.**

About the faculty

Ted Cohen, MS, CCE, FACCE
Clinical Engineering Consultant

- Part-time clinical engineering consultant. Projects include assisting VA HTM staff in VISN20 (Pacific Northwest) connect medical devices to the new VA Cerner EHR.
- For more than 35 years Manager of Clinical Engineering (now retired) at UC Davis Health in Sacramento CA, responsible for medical technology planning, and management of medical equipment installation, repair and maintenance services.
- Adjunct Professor (mostly retired), Electronics Technology, American River College. Developed a new BMET education program for a local community college district and co-taught some of its courses.
- Author of AAMI's Computerized Maintenance Management Systems for Clinical Engineering/HTM.
- Author of several CE articles and presentations on CMMS, benchmarking medical equipment services, and the integration of information technology and medical systems.
- ACCE News Managing Editor

Agenda/Learning Objectives

Information Technology 1 (September 20)

- Introduction to Medical Device Interoperability and Device Integration
- Clinical Systems Networking and Networking 101
- Wireless
- Integration of Medical Device Data with HL-7

Information Technology 2 (September 27)

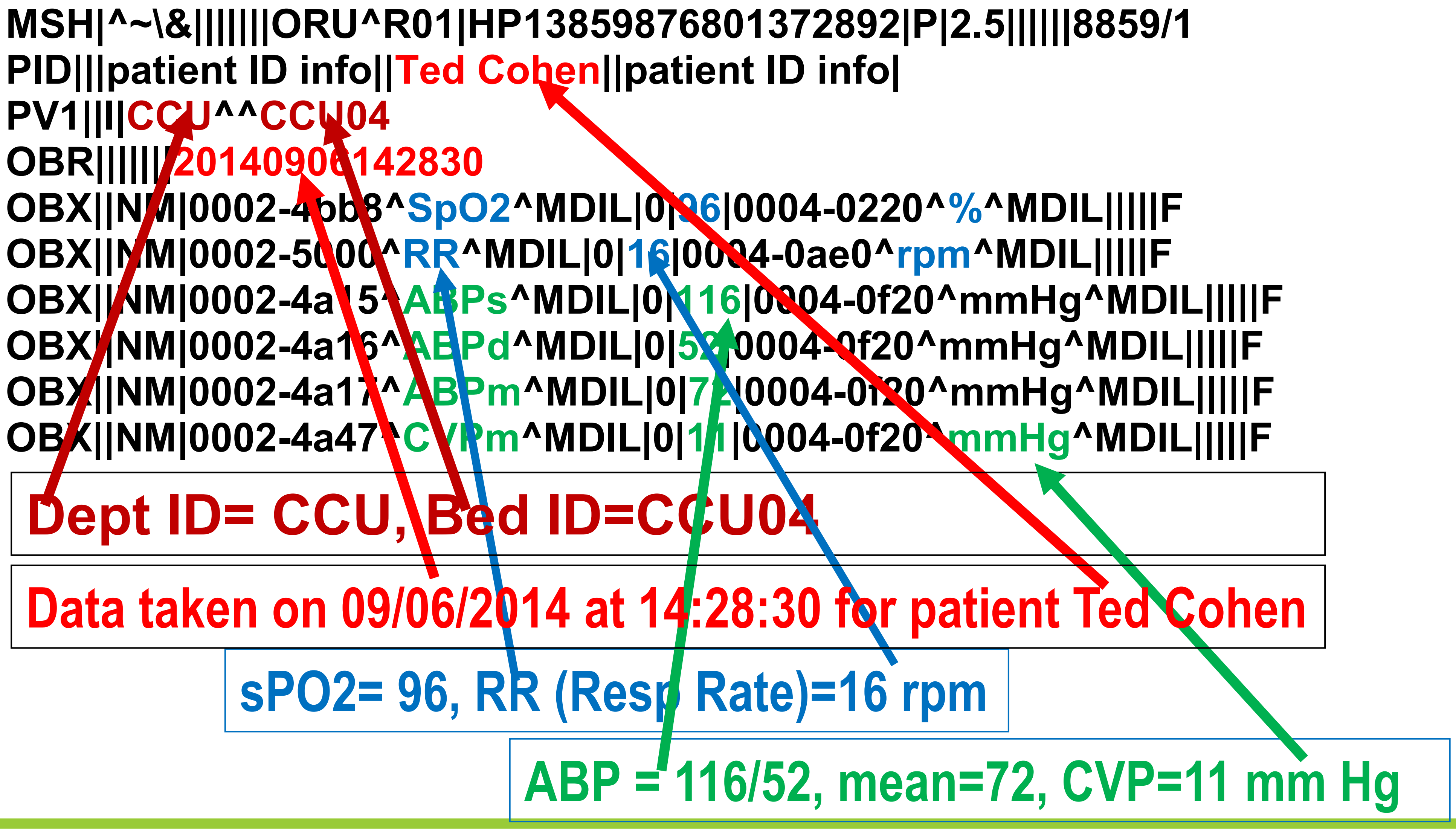
- Quick review
- HL-7 continued
- DICOM
- Cybersecurity
- Confidentiality/HIPAA
- IT Service Management
- IT Other

Integration of Medical Device Data Continued

Quick Review of IT-1 Medical Device Integration

- **Why integration of Medical Devices?**
  - Data for the next clinical decision
  - Importance of clinical staff workflow optimization
- **Network architecture**
  - One physical network with **logical** separation
- **HL-7: Integration standard for medical data**

Review: HL-7 Patient Monitor Data Example



```
MSH|^~\&|||||||ORU^R01|HP13859876801372892|P|2.5||||||8859/1
PID|||patient ID info||Ted Cohen||patient ID info|
PV1|||I|CCU^^CCU04
OBR|||||||20140906142830
OBX||NM|0002-4bb8^SpO2^MDIL|0|96|0004-0220^%^MDIL|||||F
OBX||NM|0002-5000^RR^MDIL|0|16|0004-0ae0^rpm^MDIL|||||F
OBX||NM|0002-4a15^ABPs^MDIL|0|116|0004-0f20^mmHg^MDIL|||||F
OBX||NM|0002-4a16^ABPd^MDIL|0|52|0004-0f20^mmHg^MDIL|||||F
OBX||NM|0002-4a17^ABPm^MDIL|0|72|0004-0f20^mmHg^MDIL|||||F
OBX||NM|0002-4a47^CVPm^MDIL|0|11|0004-0f20^mmHg^MDIL|||||F
```

Dept ID= CCU, Bed ID=CCU04

Data taken on 09/06/2014 at 14:28:30 for patient Ted Cohen

sPO2= 96, RR (Resp Rate)=16 rpm

ABP = 116/52, mean=72, CVP=11 mm Hg

Go over HL-7 exercise:

1. What version of HL7 is this clip from?

2. What is the patient’s name?

3. At what time was (patient name’s) heart rate taken?

4. What is (patient name’s) non-invasive blood pressure?

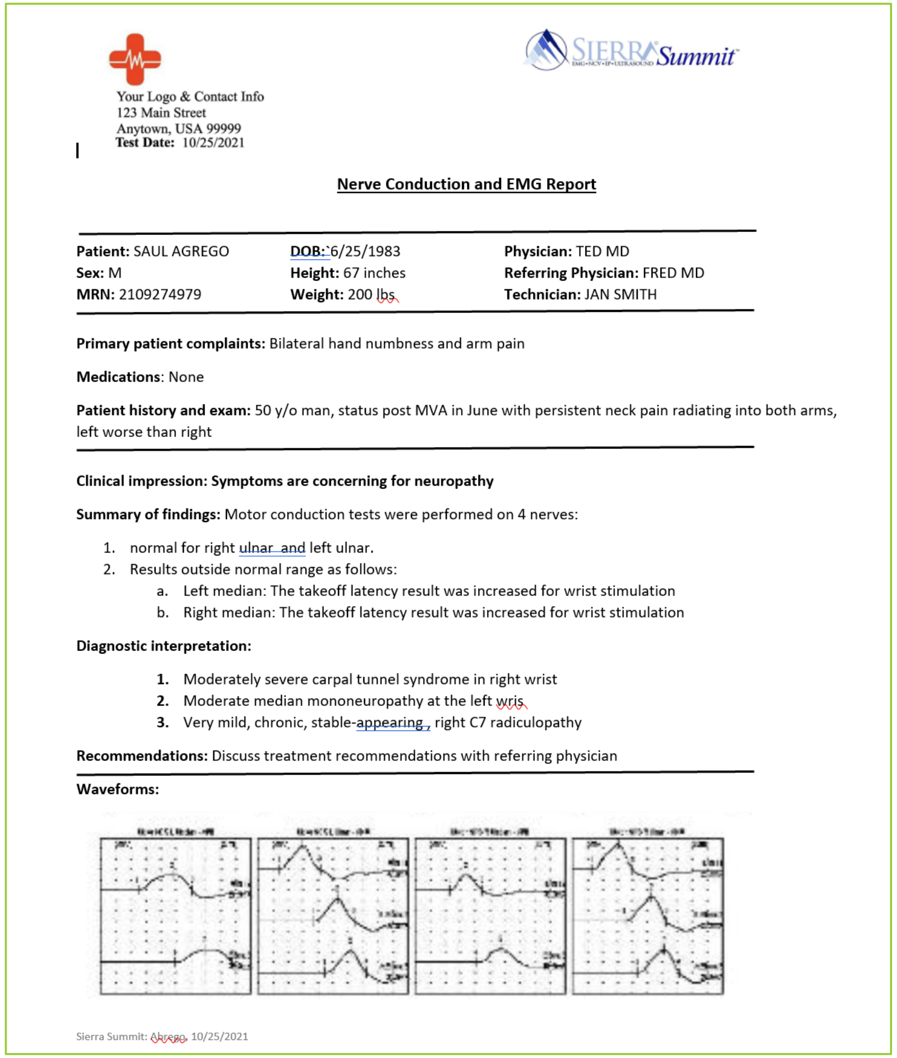
5. What time was NBP taken?

6. What is (patient name’s) end-tidal CO2?, What units?

```
MSH|^~\&|||||||ORU^R01|HP104220879017992|P|2.4|||||8859/1<CR>
PID|||MRN5733^^^^MR||Smith^John|Jones^Fran|19550508|M<CR>
PV1||I|^^Doc1&5&1<CR>
OBR|||||||20120110152630<CR>
OBX||NM|0002-4bb8^SpO2^MDIL|0|95|0004-0220^%^MDIL|||||F<CR>
OBX||NM|0002-5000^Resp^MDIL|0|15|0004-0ae0^rpm^MDIL|||||F<CR>
OBX||NM|0002-4182^HR^MDIL|0|60|0004-0aa0^bpm^MDIL|||||F<CR>
OBX||NM|0002-4a15^ABPs^MDIL|0|120|0004-0f20^mmHg^MDIL|||||F<CR>
OBX||NM|0002-4a16^ABPd^MDIL|0|70|0004-0f20^mmHg^MDIL|||||F<CR>
OBX||NM|0002-4a17^ABPm^MDIL|0|91|0004-0f20^mmHg^MDIL|||||F<CR>
OBX||NM|0002-4a05^NBPs^MDIL|0|120|0004-
0f20^mmHg^MDIL|||||F||APERIODIC|20120110152610<CR>
OBX||NM|0002-4a06^NBPd^MDIL|0|80|0004-
0f20^mmHg^MDIL|||||F||APERIODIC|20120110152610<CR>
OBX||NM|0002-4a07^NBPm^MDIL|0|90|0004-
0f20^mmHg^MDIL|||||F||APERIODIC|20120110152610<CR>
OBX||NM|0002-50b0^etCO2^MDIL|0|7.08|0004-0220^%^MDIL|||||F<CR>
```

HL-7: Widely used to transmit data from many types of medical devices

- Physiological monitors (e.g., ICU)
- Telemetry and vital sign monitors
- Anesthesia machines
- Ventilators
- Clinical lab instrumentation
- EEG, EMG, Sleep and other Neurology systems
- pdf reports including waveform clips →
- OR systems (e.g., heart/lung bypass systems)
- Infusion pump management
- "Smart" Medication cabinets



Your Logo & Contact Info
123 Main Street
Anytown, USA 99999
Test Date: 10/25/2021

Nerve Conduction and EMG Report

Patient: SAUL AGREGO	**DOB:**`6/25/1983	**Physician:** TED MD
Sex: M	**Height:** 67 inches	**Referring Physician:** FRED MD
MRN: 2109274979	**Weight:** 200 lbs	**Technician:** JAN SMITH

Primary patient complaints: Bilateral hand numbness and arm pain

Medications: None

Patient history and exam: 50 y/o man, status post MVA in June with persistent neck pain radiating into both arms, left worse than right

Clinical impression: Symptoms are concerning for neuropathy

Summary of findings: Motor conduction tests were performed on 4 nerves:

1. normal for right ulnar and left ulnar.
2. Results outside normal range as follows:
   a. Left median: The takeoff latency result was increased for wrist stimulation
   b. Right median: The takeoff latency result was increased for wrist stimulation

Diagnostic interpretation:

1. Moderately severe carpal tunnel syndrome in right wrist
2. Moderate median mononeuropathy at the left wris
3. Very mild, chronic, stable-appearing , right C7 radiculopathy

Recommendations: Discuss treatment recommendations with referring physician

Waveforms:

Sierra Summit: Abrego, 10/25/2021

HL-7 Testing

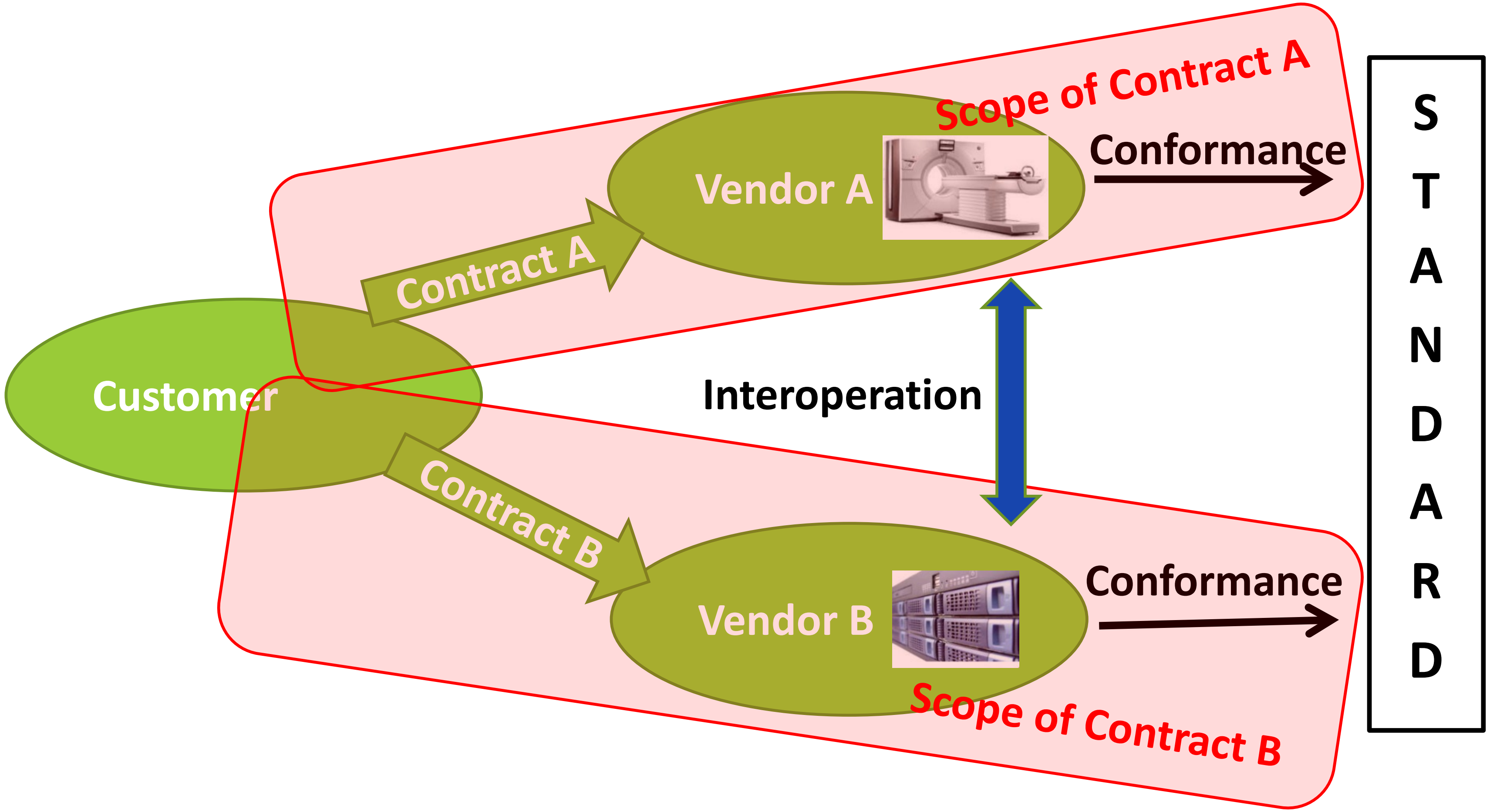
- Version alignment
- Vendor conformance statement
- Vendor interpretation and customization (e.g., patient id)
- Version 2 has the most significant use by far (since 1990)
- Most interfaces > 80% standard, < 20% custom but often some custom
- “Framework for negotiation”, not a very stringent standard

HL-7: Examples of HL-7 technical issues

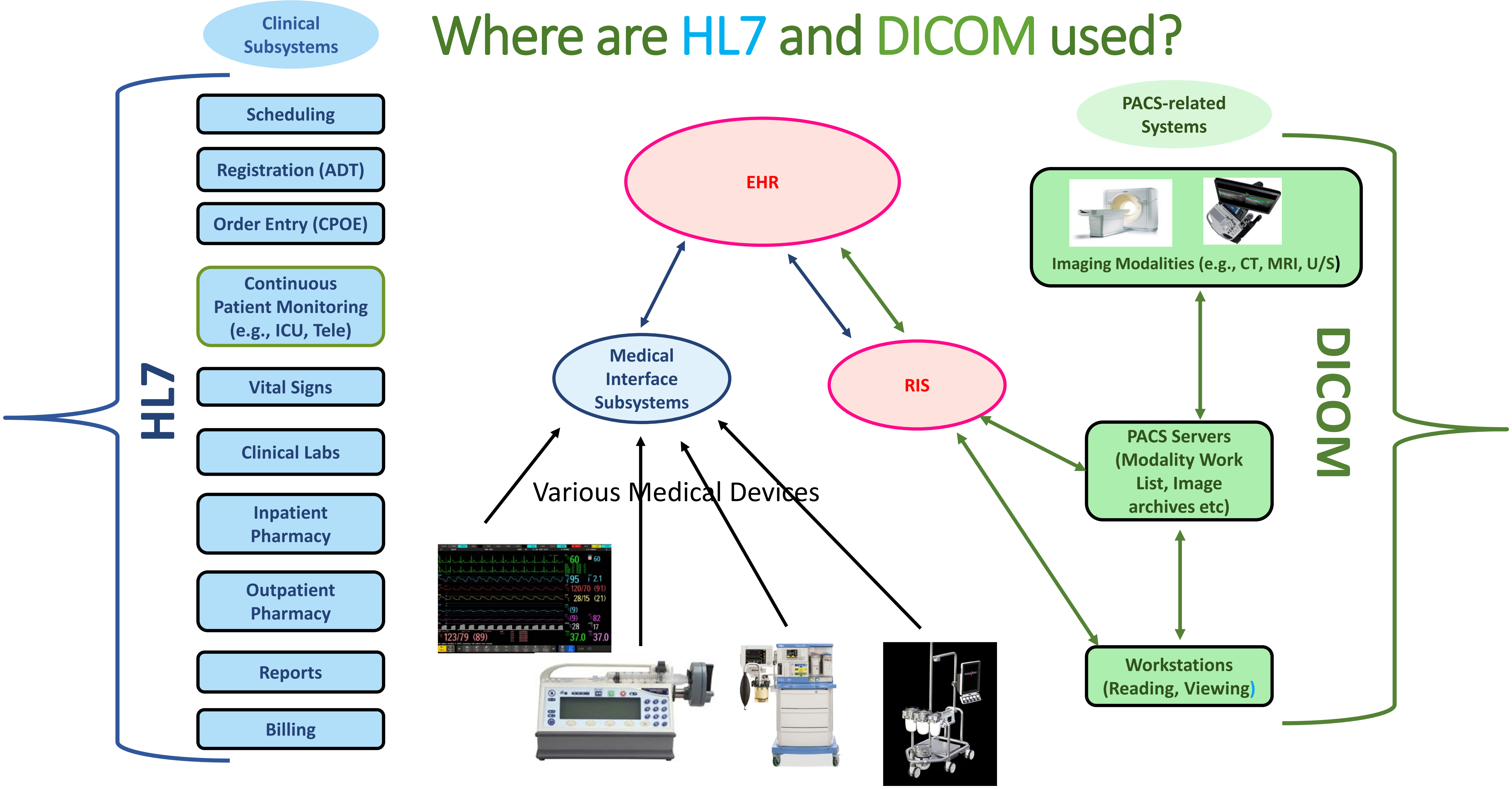
- HL-7 version and configuration management
- Configuration (making sure the settings on each product match within their limited HL-7 capabilities)
- Time Sync (message time can be off from various devices’ clocks, so need to use NTP or some other time sync protocol)
- Multiple patient ID workflows (e.g., some systems still use bed labels if the patient’s name is optional within the HL-7 data coming from the patient monitoring system)
- Parameter matching (e.g., ABP is not the same as ART)

Integration of medical device data: DICOM

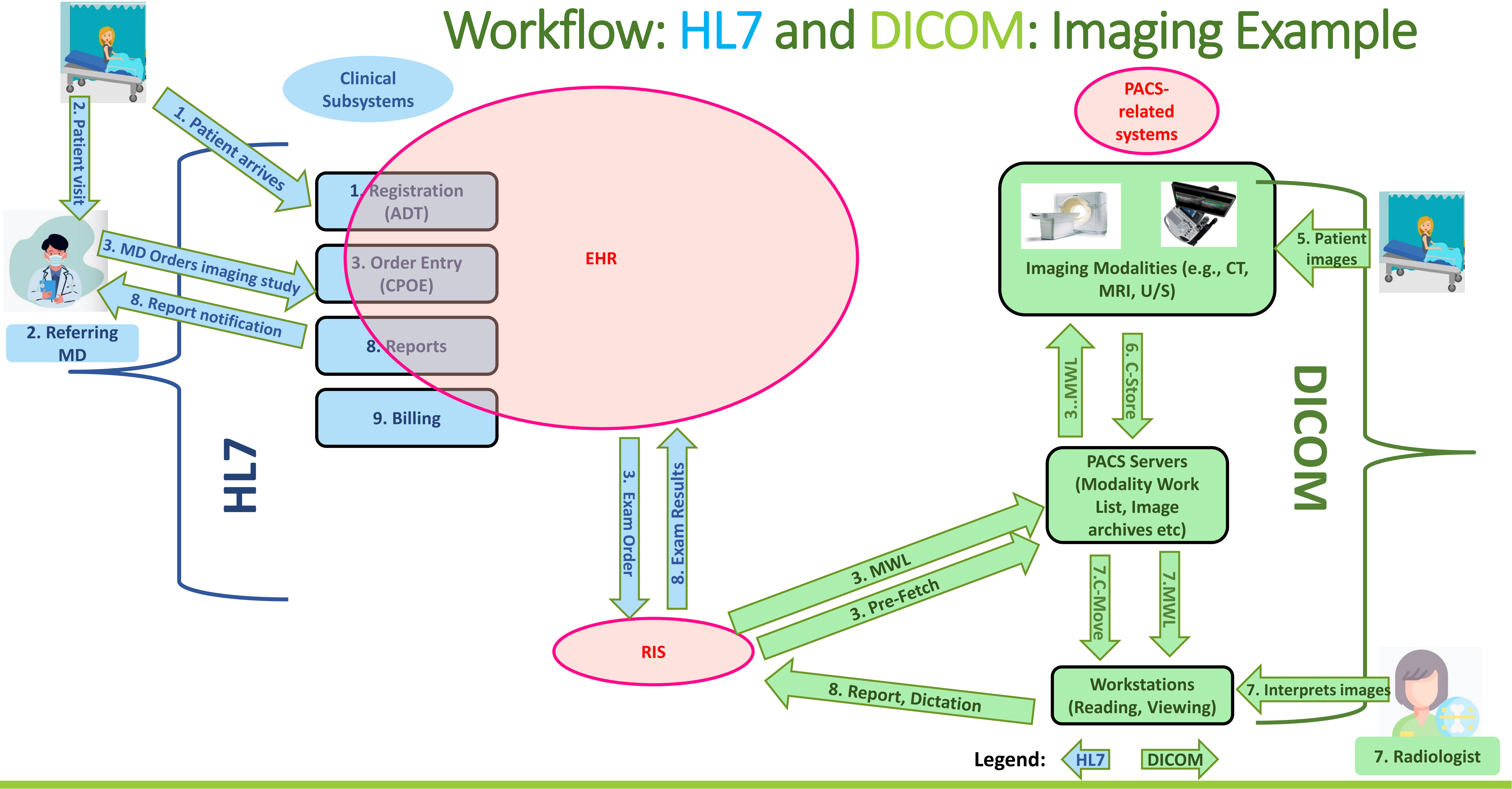
Data communication standards provide multi-vendor communication capability



Where are HL7 and DICOM used?



Workflow: HL7 and DICOM: Imaging Example



Clinical Subsystems

1. Patient arrives

2. Patient visit

2. Referring MD

3. MD Orders imaging study

8. Report notification

1. Registration (ADT)

3. Order Entry (CPOE)

8. Reports

9. Billing

EHR

HL7

3. Exam Order

8. Exam Results

RIS

3. MWL

3. Pre-Fetch

8. Report, Dictation

PACS-related systems

Imaging Modalities (e.g., CT, MRI, U/S)

5. Patient images

3..MWL

6. C-Store

PACS Servers (Modality Work List, Image archives etc)

7.C-Move

7.MWL

Workstations (Reading, Viewing)

7. Interprets images

7. Radiologist

DICOM

Legend: HL7 DICOM

DICOM: Digital Imaging and Communication in Medicine

- Developed by the National Electrical Manufacturers Association (NEMA) and American College of Radiology (ACR).
- Standard for the distribution and viewing of medical images across multiple vendor platforms using TCP/IP. Includes patient identifying information, worklists and images.
- Covers most image formats (e.g. X-ray, CT, MRI, Ultrasound, Rad-Onc, Pathology (microscope images), Endoscopy)

DICOM Conformance Statements

Product Name and Version

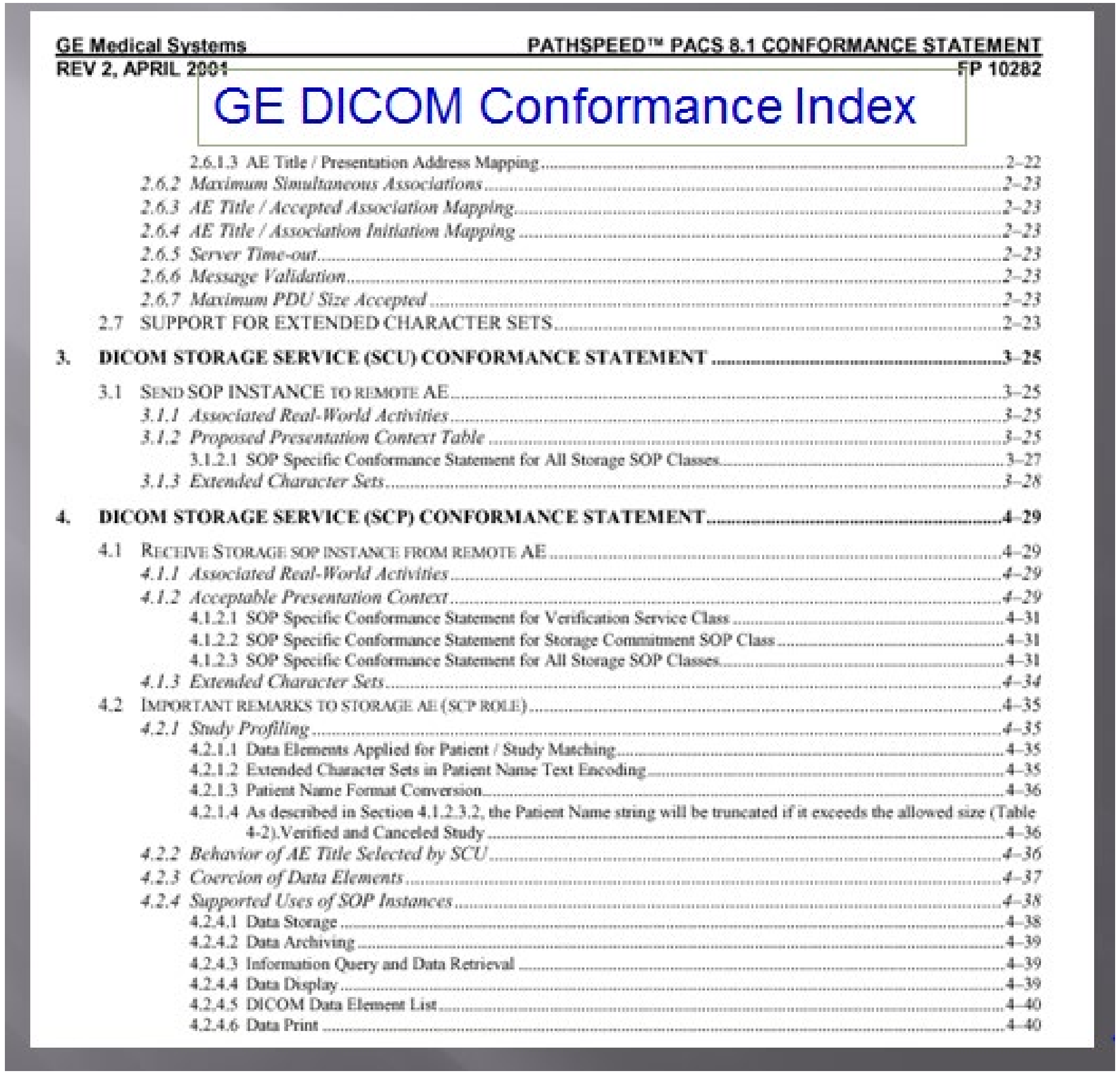
Application Data Flow Diagram

Presentation Context

Transfer Syntax

Configurable Parameters

Product Supported Data Elements
(public and private tags)



GE Medical Systems — PATHSPEED™ PACS 8.1 CONFORMANCE STATEMENT

REV 2, APRIL 2001 — FP 10282

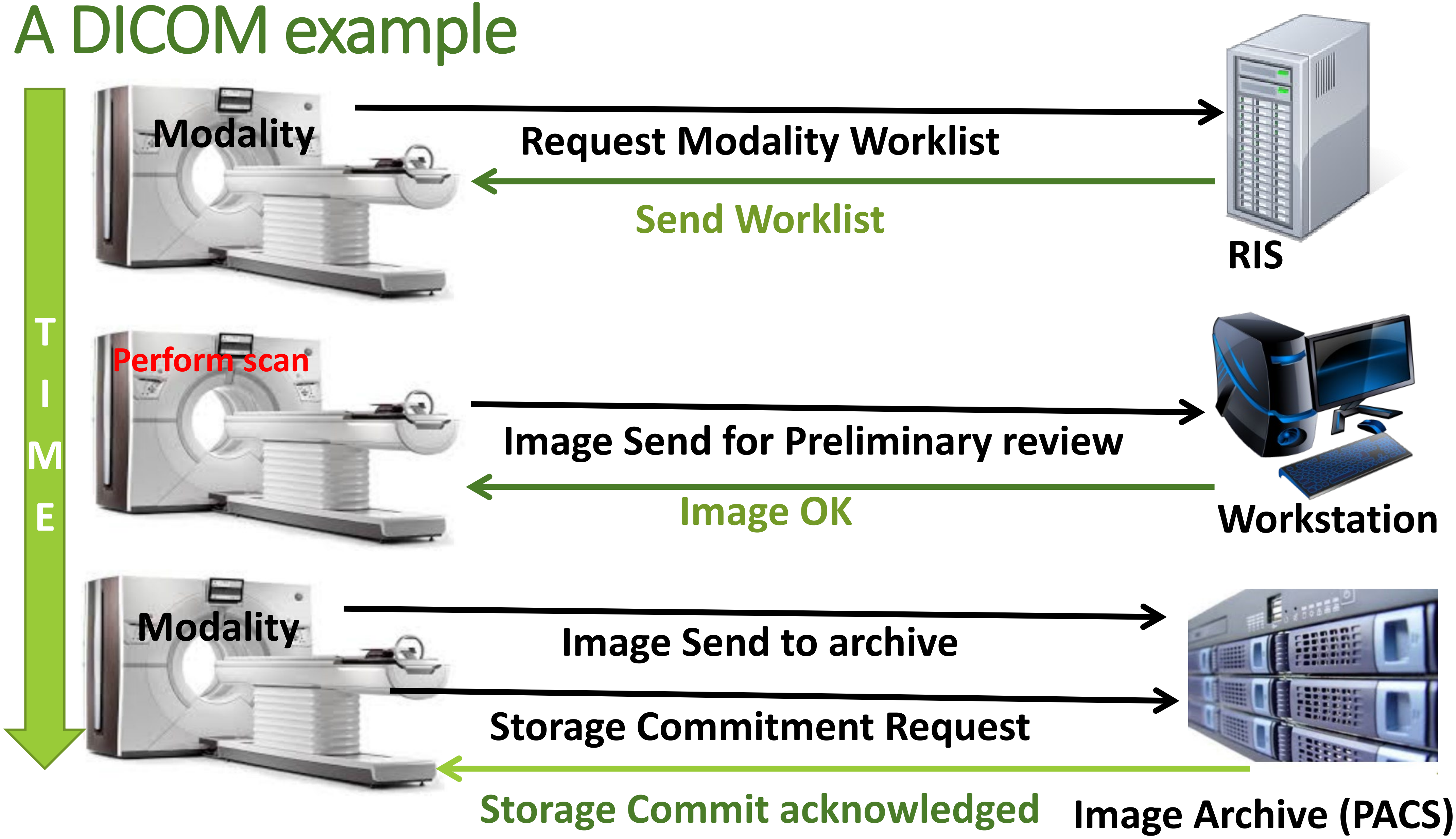
GE DICOM Conformance Index

DICOM: The AE (Application Entity) Title

- During a DICOM Association Negotiation (how two diverse products start their communication) , the products present themselves to each other using AE Titles as well as other network information (e.g., IP address, subnet mask):

- The AE Title is a 16 character (max) string that must be unique on a given network.
  - Examples: ct1, mr1805, GE_Cardiac CT

A DICOM example



TIME

Modality

Request Modality Worklist

Send Worklist

RIS

Perform scan

Image Send for Preliminary review

Image OK

Workstation

Modality

Image Send to archive

Storage Commitment Request

Storage Commit acknowledged

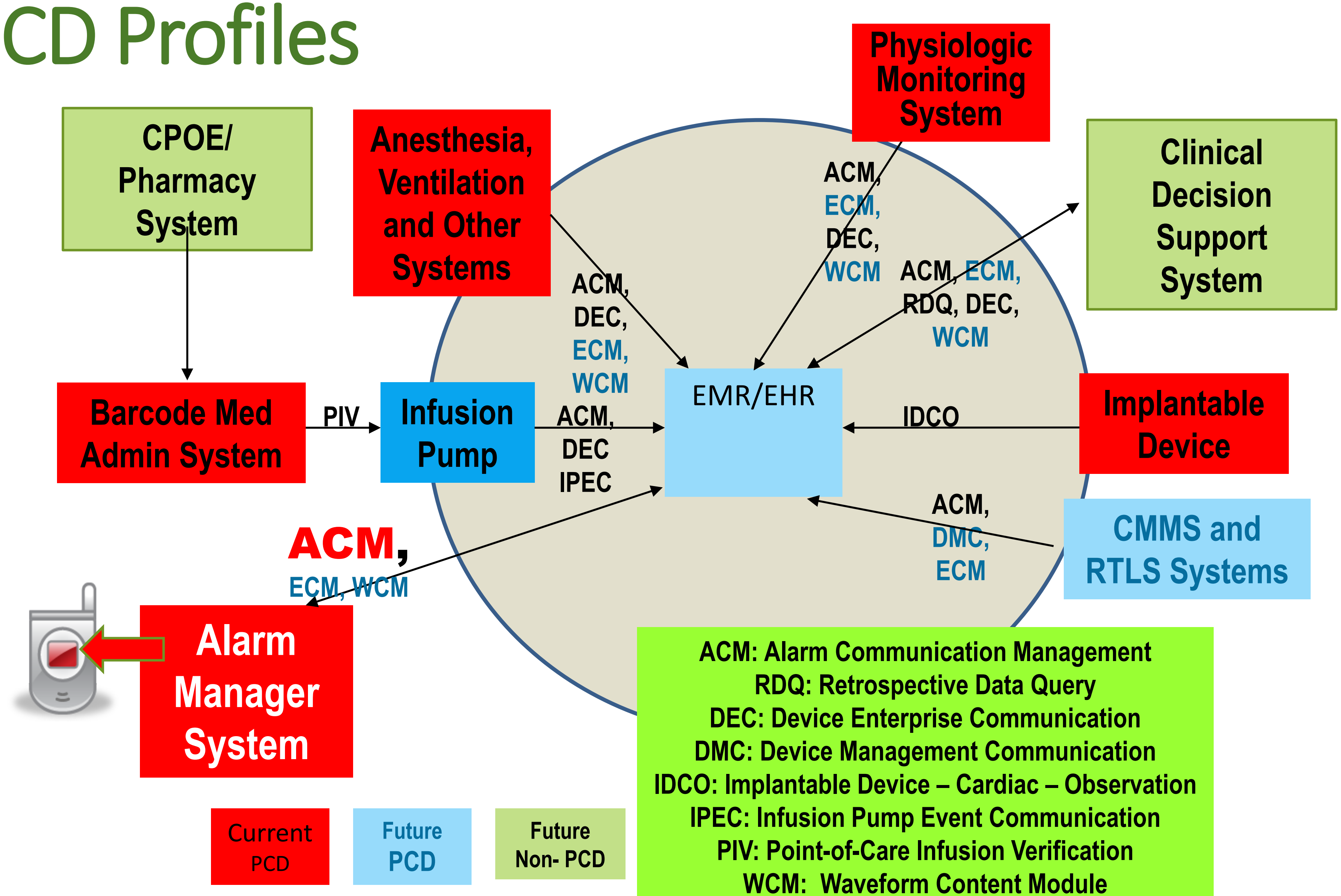
Image Archive (PACS)

IHE: Integrating the Healthcare Enterprise

- Many healthcare organizations have shown that integration of medical devices and IT systems is possible, HOWEVER:
  - Current interface standards are complex, sometimes, vague and allow too many options
  - OEMs often apply interface standards inconsistently
  - Result is “interoperability” which is vendor-dependent, complex, expensive, inefficient, and difficult to maintain.

- IHE profiles improve standards by adding consistency and eliminating or reducing options

IHE PCD Profiles



CPOE/ Pharmacy System

Barcode Med Admin System

PIV

Infusion Pump

ACM, DEC IPEC

Anesthesia, Ventilation and Other Systems

ACM, DEC, ECM, WCM

Physiologic Monitoring System

ACM, ECM, DEC, WCM

Clinical Decision Support System

ACM, ECM, RDQ, DEC, WCM

EMR/EHR

Implantable Device

IDCO

CMMS and RTLS Systems

ACM, DMC, ECM

Alarm Manager System

ACM, ECM, WCM

🟥	🟦	🟩
Current PCD	Future PCD	Future Non- PCD

ACM: Alarm Communication Management
RDQ: Retrospective Data Query
DEC: Device Enterprise Communication
DMC: Device Management Communication
IDCO: Implantable Device – Cardiac – Observation
IPEC: Infusion Pump Event Communication
PIV: Point-of-Care Infusion Verification
WCM: Waveform Content Module

From AAMI 2014 Annual Meeting: **AAMI-HTF's Managing Risks of Integrated Systems and Networks in Healthcare Environments**

IHE: 2 Example profiles: ACM and DEC

- [ACM] Alert Communication Management enables the remote communication of point-of-care medical device alert conditions ensuring the right alert with the right priority to the right individuals with the right content (e.g., evidentiary data). It also supports alarm escalation or confirmation based on dissemination status, such as whether the intended clinician has received and acknowledged the condition.

- [DEC] Device Enterprise Communication supports publication of information acquired from point-of-care medical devices to applications such as clinical information systems and electronic health record systems, using a consistent messaging format and device semantic content.

Reference: https://www.ihe.net/ihe_domains/devices/

Other data integration standards: FHIR

- FHIR (Fast Healthcare Interoperability Resources)
  - Next generation standards framework created by HL-7 organization
  - Combines the best features of HL-7 v2, HL-7 v3, and CDA (HL7"s Clinical Document Architecture)
  - Leverages the latest web standards, focus on implementability, using building blocks called "Resources"
  - Interfaces built "at a fraction of the price of existing resources"
  - Suitable for use in a variety of healthcare contexts including: mobile phone apps, cloud communications, EHR data-sharing, and much more.
  - Not necessarily focused on medical devices ("afterthought")

CCE Review Course

CYBERSECURITY FOR NETWORKED MEDICAL DEVICES

Cyber attacks: Are medical devices vulnerable?

Researchers have found that:

- Thousands of critical medical systems are accessible to hackers online.
- One study: 68,000 medical systems from a large unnamed US health group were found to be “exposed”

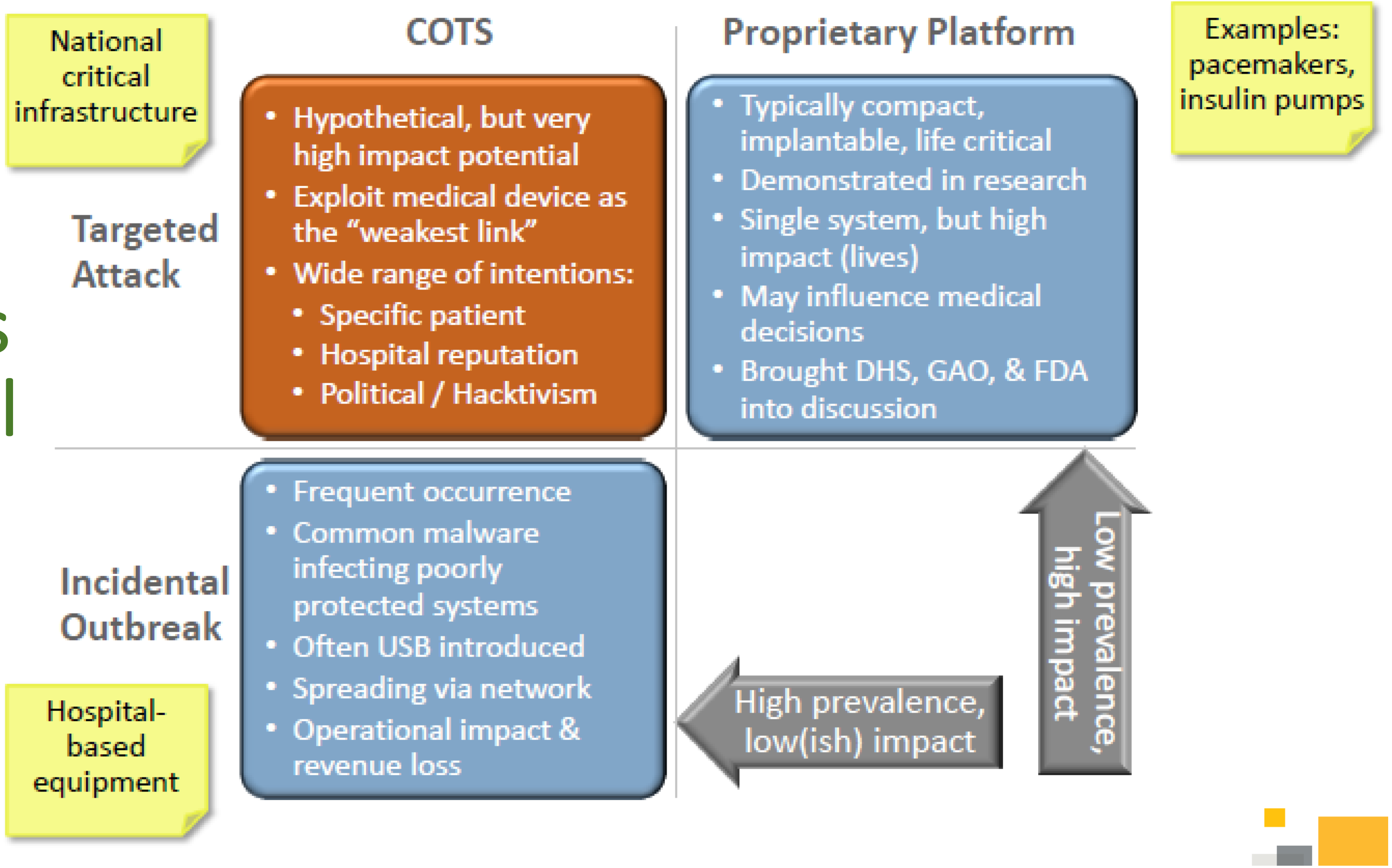
Thousands of “misconfigurations and direct attack vectors“ were found.

Researchers set up software that mimicked an MRI and a defibrillator, put them on line and found:

- “Tens of thousands of log on attempts, 299 attempts to install malware”

Reference: https://www.bbc.com/news/technology-34390165

Security infection scenarios: Intentional vs Unintentional



National critical infrastructure

COTS

Proprietary Platform

Examples: pacemakers, insulin pumps

Targeted Attack

COTS:
- Hypothetical, but very high impact potential
- Exploit medical device as the “weakest link”
- Wide range of intentions:
  - Specific patient
  - Hospital reputation
  - Political / Hacktivism

Proprietary Platform:
- Typically compact, implantable, life critical
- Demonstrated in research
- Single system, but high impact (lives)
- May influence medical decisions
- Brought DHS, GAO, & FDA into discussion

Incidental Outbreak

COTS:
- Frequent occurrence
- Common malware infecting poorly protected systems
- Often USB introduced
- Spreading via network
- Operational impact & revenue loss

Hospital-based equipment

High prevalence, low(ish) impact

Low prevalence, high impact

Courtesy of Axel Wirth: MedCrypt, San Diego CA

Cybersecurity: Medical device specific challenges

- Regulatory guidelines (e.g., FDA, CMS, TJC)
- Long life, resulting in obsolete systems (e.g., obsolete OS)
- High complexity
- Manufacturer not focused on security (changing)
- Unable to use standard IT security tools (e.g., can’t load agents)
- Lateral attacks (poorest protected surface) resulting in unintentional malware infections
- Often require manual, resource intensive solutions (e.g., patching)

- Need “Defense in Depth”

Cybersecurity: A few more IT definitions

- DNS: Domain Name Service: An IT infrastructure service that translates Host names and URLs to IP addresses.

- NAT: Network Address Translation: NAT is a process where a network device, usually a firewall, assigns a public address to a computer inside a private network.

- VPN: A Virtual Private Networks extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

- VM: Virtual Machine: A VM is a software application that performs most functions of a physical computer, actually behaving as a separate computer system. It allows one physical computer (host) to act as multiple computers even allowing different operating systems on each virtual computer. The control system, or supervising software, for the VM is called a “hypervisor”.

NIST Cybersecurity Framework

Function	Category
Identify	Asset Management
	Business Environment
	Risk Assessment, Risk Management Strategy
Protect	Access Control
	Awareness and training
	Data Security, Data Protection Processes and Protective Technology
	Maintenance
Detect	Anomalies and Events
	Continuous Security Monitoring
	Detection Processes
Respond	Response Planning
	Communication
	Analysis
	Mitigation and Improvements
Recover	Recovery Planning, Improvements, Communication

Reference: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology February 12, 2014

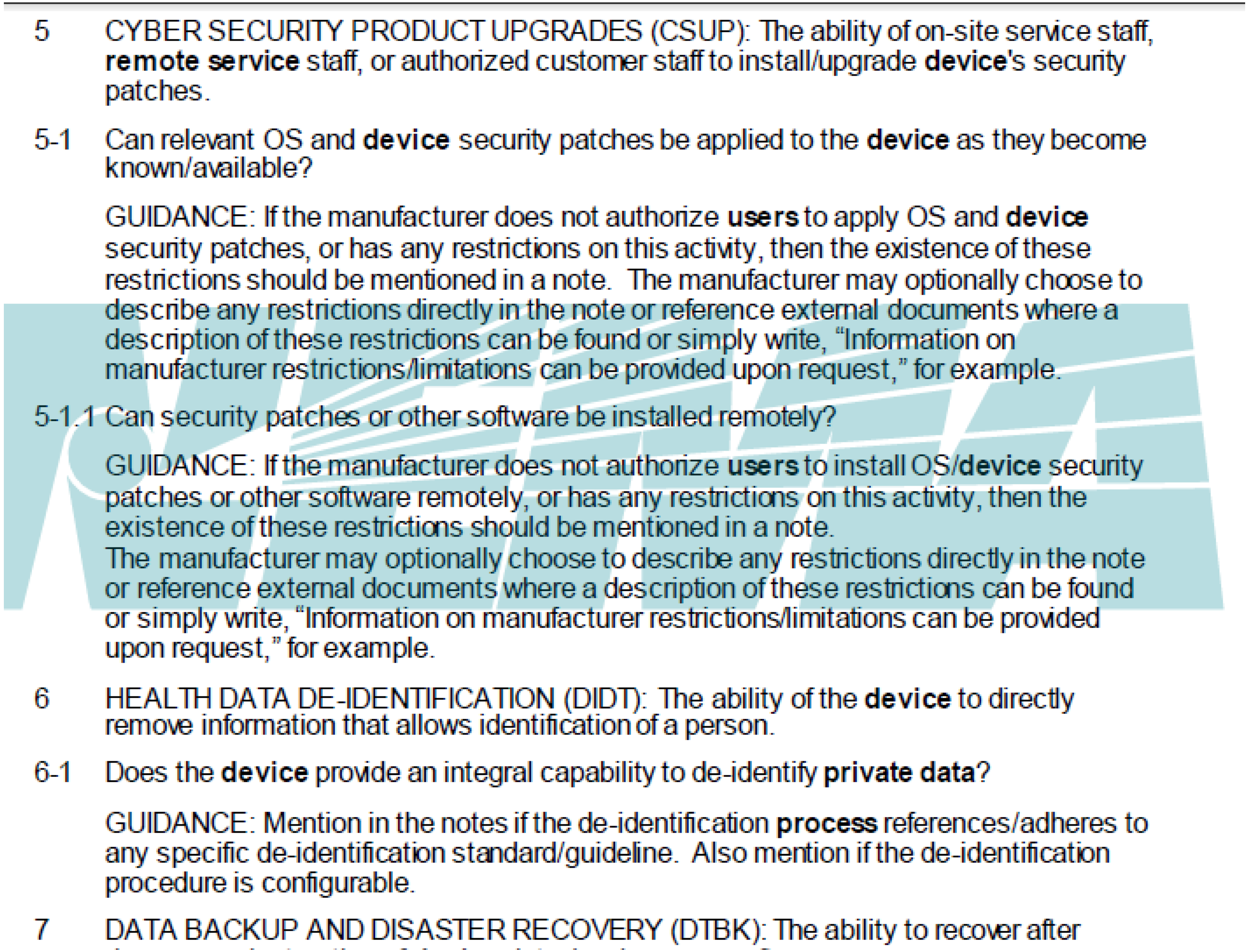
Function

Identify

Cybersecurity: Asset Management

- Inventory: Identify network-connected medical devices
- Collect MDS^2 and SBoM (software bill of materials) for identified devices
- Document in CMMS, CMDB and/or elsewhere
- Need defined process for assessing security risks of new (and existing) network-connected devices
- Establish minimum requirements for new network connected medical devices

NEMA Manufacturer Disclosure Statement for Medical Devices (MDS^2)



5 CYBER SECURITY PRODUCT UPGRADES (CSUP): The ability of on-site service staff, **remote service** staff, or authorized customer staff to install/upgrade **device**'s security patches.

5-1 Can relevant OS and **device** security patches be applied to the **device** as they become known/available?

GUIDANCE: If the manufacturer does not authorize **users** to apply OS and **device** security patches, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note. The manufacturer may optionally choose to describe any restrictions directly in the note or reference external documents where a description of these restrictions can be found or simply write, "Information on manufacturer restrictions/limitations can be provided upon request," for example.

5-1.1 Can security patches or other software be installed remotely?

GUIDANCE: If the manufacturer does not authorize **users** to install OS/**device** security patches or other software remotely, or has any restrictions on this activity, then the existence of these restrictions should be mentioned in a note.
The manufacturer may optionally choose to describe any restrictions directly in the note or reference external documents where a description of these restrictions can be found or simply write, "Information on manufacturer restrictions/limitations can be provided upon request," for example.

6 HEALTH DATA DE-IDENTIFICATION (DIDT): The ability of the **device** to directly remove information that allows identification of a person.

6-1 Does the **device** provide an integral capability to de-identify **private data**?

GUIDANCE: Mention in the notes if the de-identification **process** references/adheres to any specific de-identification standard/guideline. Also mention if the de-identification procedure is configurable.

7 DATA BACKUP AND DISASTER RECOVERY (DTBK): The ability to recover after

Reference:
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx?key=67ri900e6rt5af#download

Function

Identify

Cybersecurity: Asset Management

Fields to collect:

- IP address
- MAC address
- OS name and version
- Application(s) name(s) and version(s) (SBoM)
- Physical data port ID
- AE Title for DICOM
- HIPAA info (e.g., Does the device/system store ePHI?)
- And many more

Function

Identify

Cybersecurity: Asset Management

Minimum requirements for new network connected medical devices:

- Review MDS2
- Review SBoM
- Supported OS that receives routine OS security patches
- Anti-virus applied and periodically updated
- Security patches for all applications including third-party apps
- No default “hard-coded” passwords
- Uses LDAP, Active Directory or other approved account management system
- Document any security weaknesses and work with vendor to mitigate

Cybersecurity: Risk assessment and risk management strategy

Function

Identify

Identify systems that are critical to business continuity

- Examples: Data center

Identify systems that are vulnerable

- Examples: Can’t patch, **”zero day”** delays, obsolete, FDA regulated and no approval from manufacturer to patch

Function

Identify

Cybersecurity: Asset Management

- New automated systems are available to passively discover and automatically inventory network connected assets without installing any agents.
- These systems can collect, classify, and profile the devices and collect details such as : MAC address, make, model, serial number, OS, software versions, application inventory, patch level, port information, network traffic flow information and more.
- As an added benefit: Many of these systems can also provide utilization information.

Protect

Cybersecurity: Defense in depth (Network)

- Network design (e.g,. segmentation)
- Medical device network segment(s)
- Firewalls
  - Perimeter firewall
  - Internal firewalls between segments
- Intrusion protection systems
- Port management
  - Access control lists (ACLs)
  - Close ports not in use

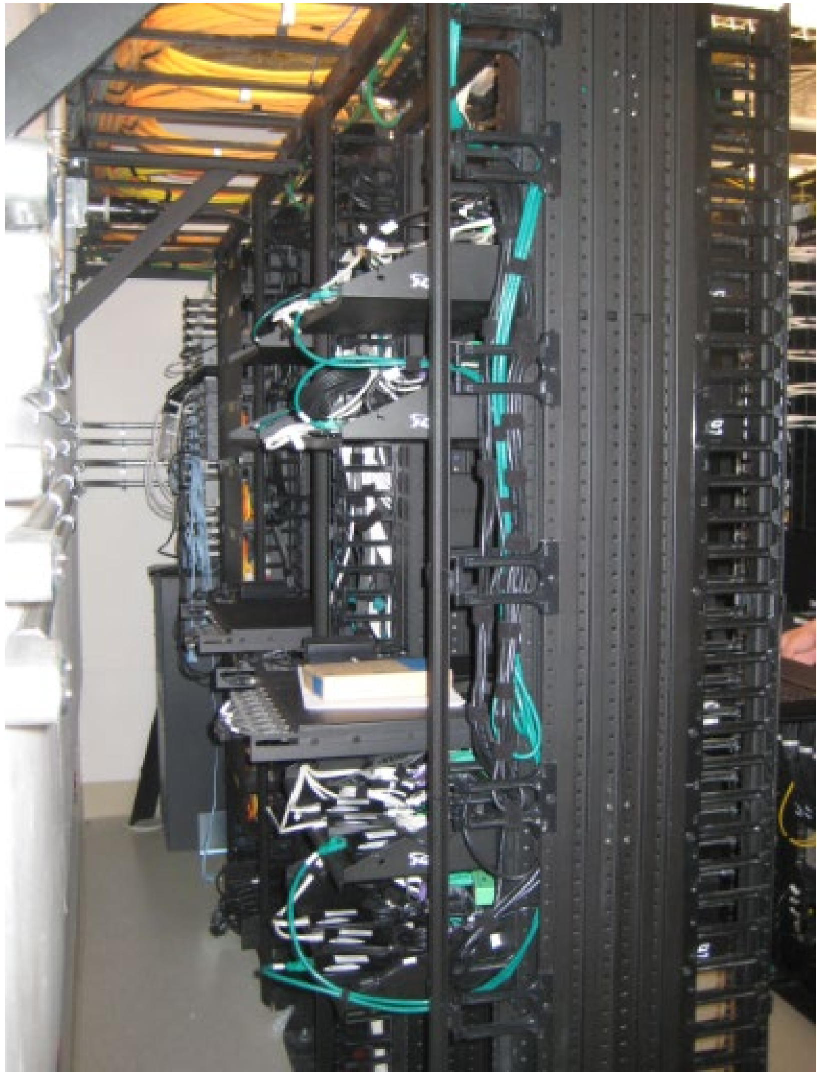
Protect

Cybersecurity: Physical security

- Card key access to data closets (IDFs)
- Block USB access
  - Or secure USB devices, password protected and encrypted (e.g. Iron Key)
- Laptops physically secured and encrypted

Cybersecurity: Physical Safeguards example

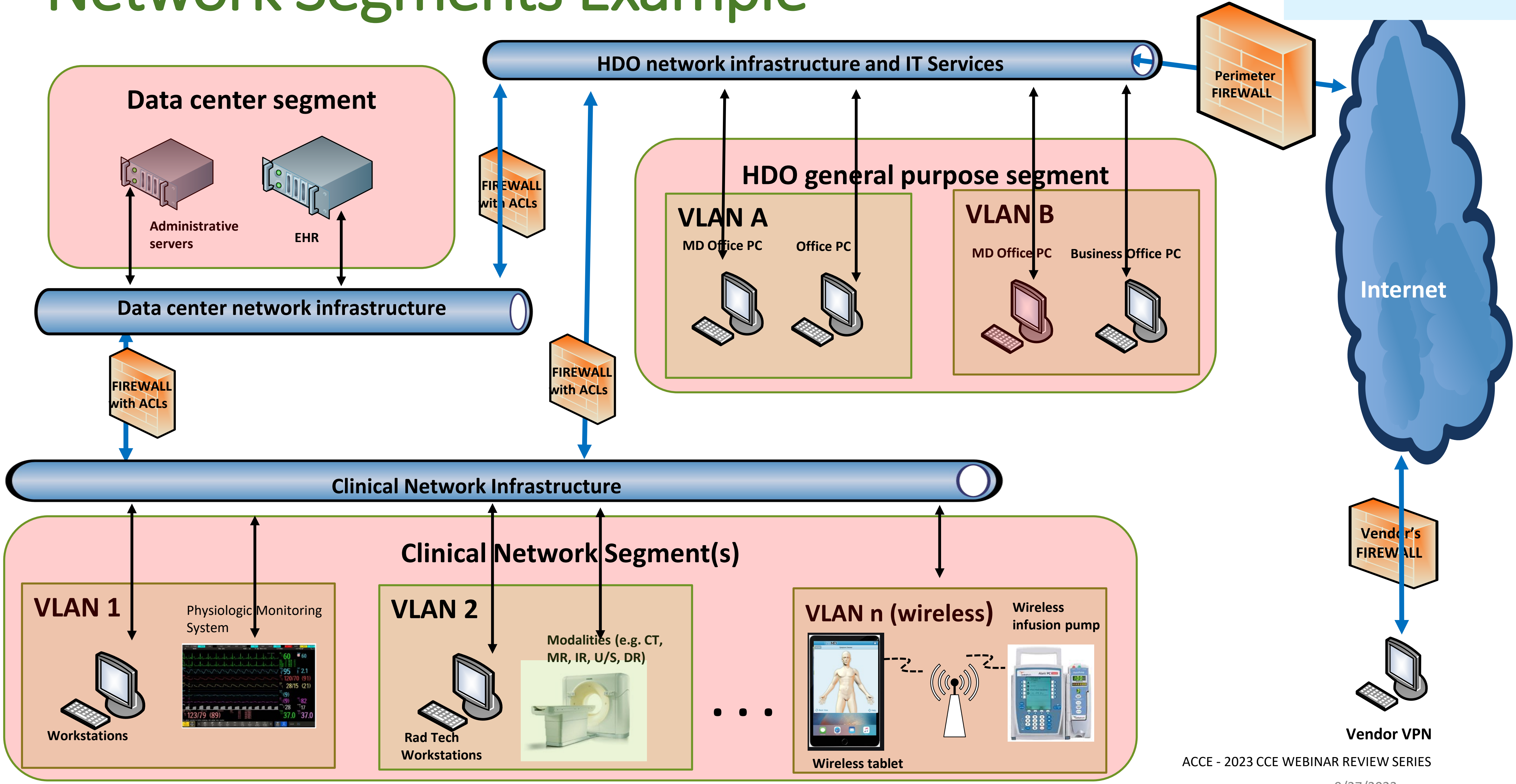
Protect



Central station computers in locked data closet

Network Segments Example

Protect



Protect

Cybersecurity: Malware protection

- Can anti-virus be installed? Which one(s), (Mfr, version?

- Any anti-virus restrictions?
  - Operational time restrictions (often these restrictions are not practical for 24x7 systems)
  - Specific program or directory restrictions
  - Other restrictions

Protect

Cybersecurity: People

- Access and control (LDAP, Active Directory)
  - Staff
  - Vendors (VPN)
  - Remote (VPN)
- Awareness and training
- Timeouts, auto logoffs
- Limited access to increase protection for sensitive data (e.g., financial, HIPAA)

Protect

Cybersecurity: User awareness

- End user training
- “Splash” page notices
- Specific communication when problems occur
- Whitelisting
- Blacklisting

Protect

Cybersecurity: HIPAA, Privacy Rule

- Regulates use and disclosure of Protected Health Information (PHI and ePHI)

- Applies to "covered entities" (Health care providers, insurers etc and their “Business Associates”

Cybersecurity: HIPAA, Privacy Rule

Protect

- Protects any information about health status and/or provision of or payment for health care, that can be linked to an individual:
  - Name, address, social security number, medical record number, drivers license etc
  - Video, photo, tattoos
- Okay to access data if you have a “need to know” (that includes CE/HTM)

Protect

Cybersecurity: HIPAA, Security rule

- Role based security
- Business Associates Agreements with vendors
- Staff training: Understand “Need to know”
- Erase/destroy ePHI when equipment is removed from use

Cybersecurity: HIPAA CIA

Protect

C

Confidentiality

Data or information is not made available or disclosed to unauthorized persons or processes.

I

Integrity

Data or information have not been **altered or destroyed** in an unauthorized manner.

A

Availability

Data or information is accessible and useable upon demand by an authorized person.

Protect

Cybersecurity: HIPAA Technical Safeguard examples

- Encryption (data at rest and data in motion)
- Remove/disable USB drives
  - or use secure encrypted USB drives (e.g., Iron Key)
- Multi-factor authentication
- LDAP (e.g., Active Directory)

Protect

Cybersecurity: HIPAA Data Integrity examples

- Right data to the right patient
- Patient safety in applications (e.g., DERS)
- Clinician confirmation of automated data
- Checksums and other technology-related data integrity features

Protect

Cybersecurity: HIPAA Availability examples

- Timely patient data (e.g,. alarms, nurse call)
- Critical equipment uptime (planned downtime)
- Backups, failover and other redundant systems
- UPSs, emergency power

Cybersecurity: What does the FDA say in its "guidance" documents?:

Protect

- What devices does this guidance cover?
  - Devices that use OTS software, connect to a network (public or private), and need updates or patches because their OTS software has been found to be "vulnerable to virus, worms or other threats".
- FDA review:
  - Ordinarily, FDA will not need to review software patches
  - Manufacturers must validate their software changes under the Quality System regulation looking at what the change does, have evidence that the changed software meets user needs and performs to specification.

Reference: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical

Cybersecurity: What does the FDA say in its “guidance” documents?:

Protect

- When can healthcare organizations apply software patches to medical devices that don't come from the medical device manufacturer?
  - “In our (FDA) view, it is rare for healthcare organizations to have enough technical resources and information on the design of medical devices to independently maintain medical device software.” Thus, most healthcare organizations need to rely on the advice of medical device manufacturers.

- “FDA Guidance documents reiterate that security software changes (e.g., patches) do not affect FDA approval (but do require manufacturer verification and validation testing.”)

Protect

Cybersecurity priorities:

- Clinical Engineering’s priorities are often (Availability, Integrity, Confidentiality) vs IT’s priorities of Confidentiality, Integrity, Availability).

- “Tension” between Availability focus and Confidentiality focus (e.g., remote access for vendors, legacy devices)

Protect

Cybersecurity: HIPAA and HTM

- Provide Administrative, Physical and Technical Safeguards
- Administrative examples:
  - Business Associates Agreements with vendors
  - Staff training: Understand “Need to know”
  - Policies on disposal: Erase/destroy ePHI as appropriate

Cybersecurity: Vulnerability Detection

Detect

- In cooperation with IT:
  - Subscribe to cybersecurity related vulnerability/attack notification system(s) from ICS-CERT databases, device manufacturers, OS vendors (e.g., Microsoft) , your IT dept etc
  - Monitor network for anomalies, intrusions and other potentially malicious activities
- Determine applicability
- Assess risk

Cybersecurity: Patching

Identify Detect Protect

- Vulnerability applicable?
- Risk?
- Patch available?
- Patch approved for install by medical device manufacturer?
  - Yes
  - No, Patch anyway or wait for manufacturer approval?
- CE resources available for patching?

Identify Protect Detect

Cybersecurity: Automation to help CE

- Several new "agent-less" products on the market that allow:
  - Asset discovery
  - Network Micro-Segmentation
  - Passive traffic monitoring with alerts and enforcement actions
  - Automated vulnerability analysis with risk assessment
  - Patch installation automation
  - Integration with HTM's CMMS and IT's CMDB
  - Life cycle management (e.g., onboarding, vulnerability logging, change management, decommissioning)

- "Active" vulnerability scanning
  - May NOT be appropriate for certain medical devices

Repond

Cybersecurity: What to do when an event occurs

- Containment: Isolate infected system
  - Suspend internet activity
  - Remove from network
- Seek help
  - IT dept
  - Device mfr
- Communicate

Cybersecurity: Recovery and “business continuity”

Recover

- Eradicate the malware
- Restore functionality
- Test
- Remove containment
- Post incident followup
  - After action report, lessons learned/what can we do better next time
  - Cost of event

CCE Review Course

IT SERVICE MANAGEMENT

TELECOMMUNICATIONS MANAGEMENT

OTHER IT AND TELECOMMUNICATION RESPONSIBILITIES

ITIL (Information Technology Infrastructure Library)

ITIL guidance documents provide a framework for best practice IT services

Five main sections of **ITIL**:

- **Service strategy:** Portfolio, financial, customer demand, business relationships
- **Service design:** Design coordination, service catalog management, service level agreements; capacity, continuity, security and supplier/procurement management

ITIL’s five sections continued:

- **Service transition:** (e.g., upgrades; change, project, release/deployment management, asset and configuration management, validation and testing
- **Service operations** (e.g., Service desk, technical and application management, IT operations; problem, incident, event, and access management)
- **Process improvement** (e.g., improvement strategy, define what to measure, collect data, process and analyze data, present and implement improvements)

ITIL and Clinical Engineering: Pre-purchase evaluation and supplier management

- Pre-procurement technology evaluation
- Pre-procurement cybersecurity evaluation
- Pre-qualified vendors
- RFP where required/needed

ITIL and Clinical Engineering: Example pre-procurement technology evaluation questionnaire

- Questions on:
  - Application management
  - System integration
  - Network communications
  - Desktop PCs and Peripherals
  - Servers
  - EMR
  - Imaging and DICOM
  - Support options (e.g., software, hardware, inhouse, contract)

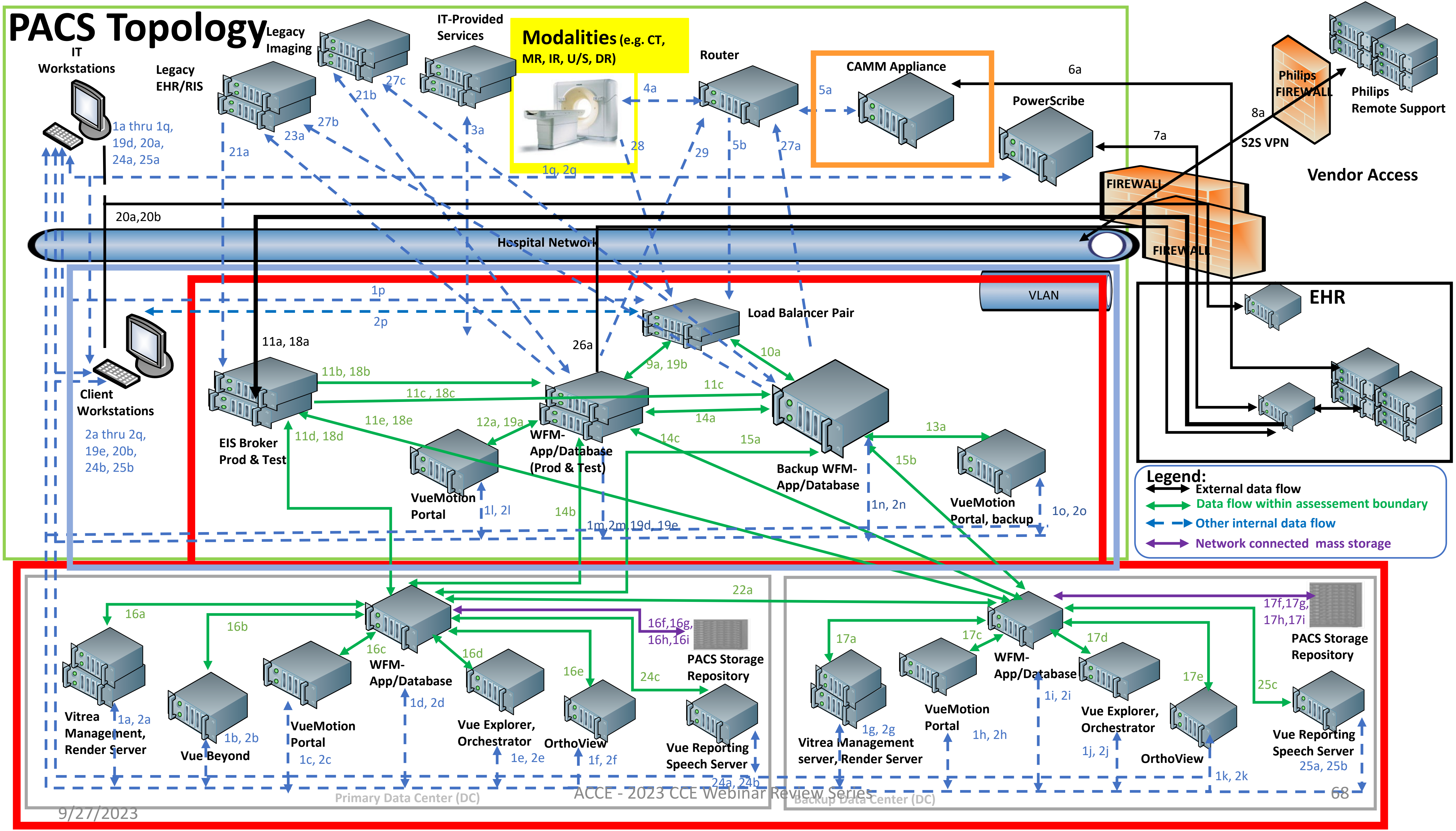
ITIL and Clinical Engineering: Example pre-procurement technology evaluation questionnaire

- Approximately 100 questions: Example questions:
  - Network: Does your application/clients able to tolerate 30ms latency at 900 miles distance? If not, please explain.
  - Data integration: What message structures are supported by the new technology for integration? (e.g., HL7 ver2, HL7 ver3, EDI, FHIR, XML) Provide a list, if other or proprietary, please specify.
  - What ports are required to be open?
  - Review SBoM

ITIL and Clinical Engineering: Example pre-procurement technology evaluation questionnaire continued

- How is patient identified in your technology? ADT or? How is the patient linked to the correct device and its data?
- Are static IP addresses required?
- Does the technology depend on IP Multicast for any functionality? If so, can it use a HDO assigned multicast group IP?
- Is external access required? Approved VPN?
- Topology diagram example available?

PACS Topology



Legend:
- External data flow
- Data flow within assessement boundary
- Other internal data flow
- Network connected mass storage

MDS^2 2019 Question Sections

Require MDS^2 2019 document or specify an additional HDO-specific security questionnaire that is similar to MDS^2 2019

- DEVICE/SYSTEM INFORMATION
- MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION
- AUTOMATIC LOGOFF (ALOF)
- AUDIT CONTROLS (AUDT)
- AUTHORIZATION (AUTH)
- CYBER SECURITY PRODUCT UPGRADES (CSUP)
- HEALTH DATA DE-IDENTIFICATION (DIDT)
- DATA BACKUP AND DISASTER RECOVERY (DTBK)
- EMERGENCY ACCESS (EMRG)
- HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)
- MALWARE DETECTION/PROTECTION (MLDP)
- NODE AUTHENTICATION (NAUT)
- CONNECTIVITY CAPABILITIES (CONN)
- PERSON AUTHENTICATION (PAUT)
- PHYSICAL LOCKS (PLOK)
- ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)
- SOFTWARE BILL OF MATERIALS (SBoM)
- SYSTEM AND APPLICATION HARDENING (SAHD)
- SECURITY GUIDANCE (SGUD)
- HEALTH DATA STORAGE CONFIDENTIALITY (STCF)
- TRANSMISSION CONFIDENTIALITY (TXCF)
- TRANSMISSION INTEGRITY (TXIG)
- REMOTE SERVICE (RMOT)
- OTHER SECURITY CONSIDERATIONS (OTHR)

ITIL: CE and team: Assess clinical workflow impact

- Review current workflow without new technology, including current practice guidelines, policies and procedures
- Identify inefficiencies that could be addressed with new system
- Review workflow with proposed technology:
  - Apply clinical scenarios
  - Identify fewer/extra steps introduced
  - Identify user-perceived challenges and how they might be mitigated (e.g., user training)

ITIL and Clinical Engineering: Installation and Release Management

- Cloud-based or on-premise (VM or specific hardware hosted)
- Test system or clinical system
- Initial (unit) testing of software as well as hardware
- Then integration testing and end-to-end system testing
- User acceptance and user training
- Command center for major releases
- Catalog initial release info in CMMS, CMDB and technical library

ITIL and Clinical Engineering: Configuration and Change Management

- Clinical Engineering representative on the Change Management Board
- Test changes before release (and regression test to make sure changes did not impact other parts of the software)
- Communications with clinical impact of change (e.g., downtime duration and plan)
- Backout plan
- Document configurations and new release info in CMMS and technical library

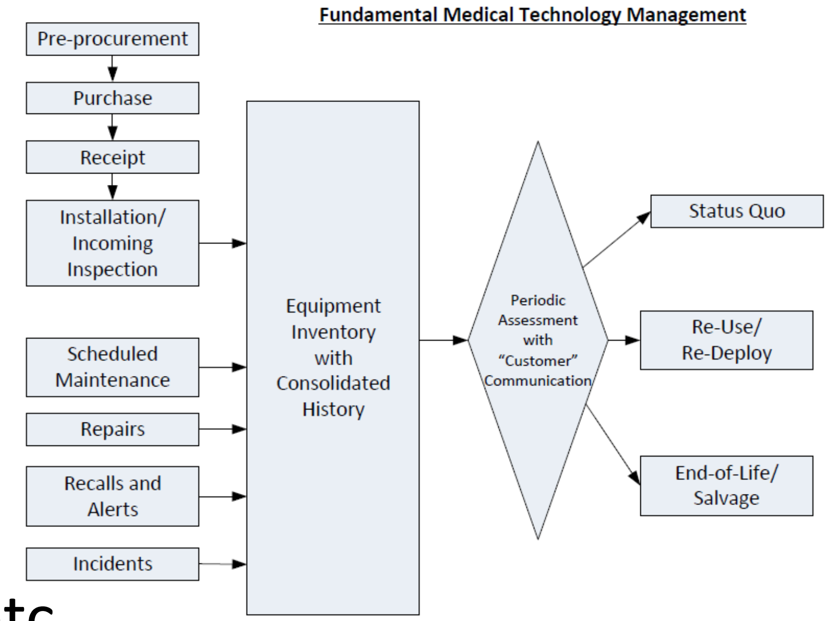
ITIL and Clinical Engineering: Help desk, dispatch, call tracking

- Network-connected medical device problems routed to CE CMMS from a common help desk (e.g., Service catalog) with the following features:
  - Help screens and Help desk scripts
  - Automated and manual dispatch, with acknowledgement
  - Call tracking with user access to status

ITIL and Clinical Engineering: Continuity and Capacity Management

- Continuity management
  - Disaster planning (e.g. backups, testing backups)
  - Disaster recovery
- Capacity Management
  - Growth planning
  - System performance metrics

Summary: Medical Equipment Management of Network Connected Devices


Fundamental Medical Technology Management

Pre-procurement

Purchase

Receipt

Installation/ Incoming Inspection

Scheduled Maintenance

Repairs

Recalls and Alerts

Incidents

Equipment Inventory with Consolidated History

Periodic Assessment with "Customer" Communication

Status Quo

Re-Use/ Re-Deploy

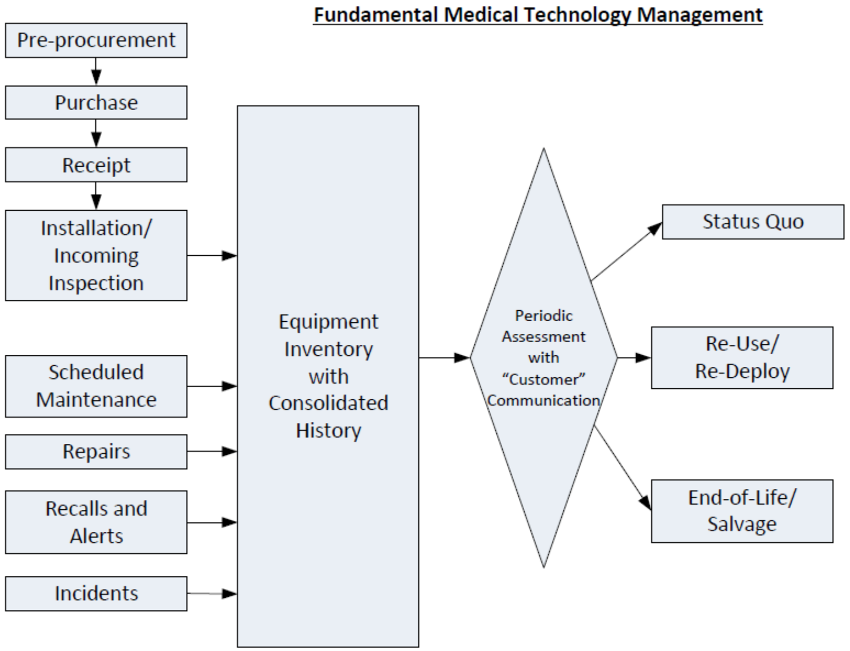
End-of-Life/ Salvage

Pre-procurement: Discovery, RFP, if needed; obtain all relevant information from manufacturer(s) to assure proposed system will work with your network, other infrastructure, cybersecurity policies, current devices etc

Purchase: Include all software, bill of materials (SBoM), security requirements, test system, tools etc

Incoming inspection/installation: Test all sub-systems. Understand and test end-to-end. Provide end user and technical training, set up remote access (e.g., VPN), document "as-builts" with IT information. Enter all info in CMDB and CMMS

Summary: Medical Equipment Management of Network Connected Devices


Fundamental Medical Technology Management
Pre-procurement
Purchase
Receipt
Installation/ Incoming Inspection
Scheduled Maintenance
Repairs
Recalls and Alerts
Incidents
Equipment Inventory with Consolidated History
Periodic Assessment with "Customer" Communication
Status Quo
Re-Use/ Re-Deploy
End-of-Life/ Salvage

Scheduled maintenance: Include routine patch management as well as required hardware maintenance

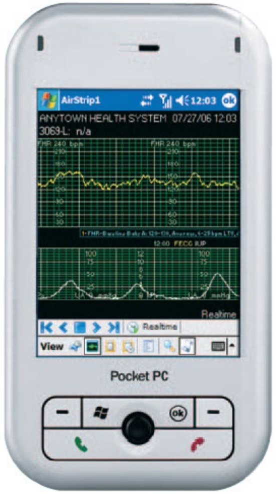
Repairs: Warranty info, vendor service contract? (SLA), include patches. Update documentation

Incidents, recalls and alerts: Include urgent patch management

Reuse/Disposal: Delete ePHI per HIPAA as appropriate

Information Technology: Telecommunications Management

- Nurse call system support
- Secondary alarm management (e.g., Vocera, nurse call, display panels/dashboards, smart phones)



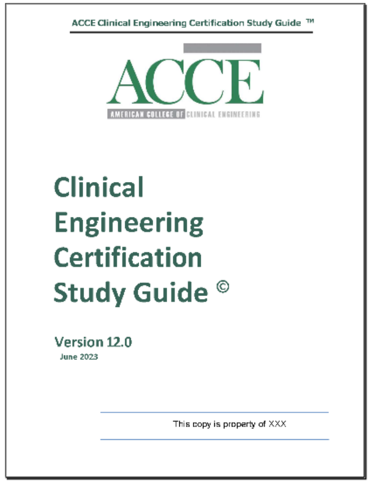
Other Telecommunications and IT Responsibilities: Telemedicine

More technology is being implemented outside of the hospital and its clinics:

- eICU
- Tele-dermatology, pathology, radiology
- Home health and IoMT: Remotely connected FDA regulated medical devices and medical-related consumer devices (e.g., glucose monitoring, fall detection, weight (CHF), medication management, exercise monitoring, “agents” for the blind)

References

- HTTPS://WWW.HL7.ORG
- HTTPS://HL7-DEFINITION.CARISTIX.COM/V2/HL7V2.3/SEGMENTS/PID
- HTTPS://WWW.IHE.NET/IHE_DOMAINS/DEVICES/
- HTTPS://WWW.BBC.COM/NEWS/TECHNOLOGY-34390165
- HTTPS://WWW.MEDCRYPT.COM/
- ITIL: HTTPS://WWW.IBM.COM/TOPICS/IT-INFRASTRUCTURE-LIBRARY
- FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FEBRUARY 12, 2014
- HTTPS://WWW.NEMA.ORG/STANDARDS/PAGES/MANUFACTURER-DISCLOSURE-STATEMENT-FOR-MEDICAL-DEVICE-SECURITY.ASPX?KEY=67RI900E6RT5AF#DOWNLOAD
- HTTPS://WWW.FDA.GOV/REGULATORY-INFORMATION/SEARCH-FDA-GUIDANCE-DOCUMENTS/INFORMATION-HEALTHCARE-ORGANIZATIONS-ABOUT-FDAS-GUIDANCE-INDUSTRY-CYBERSECURITY-NETWORKED-MEDICAL



ACCE Clinical Engineering Certification Study Guide ™

ACCE

AMERICAN COLLEGE OF CLINICAL ENGINEERING

Clinical Engineering Certification Study Guide ©

Version 12.0
June 2023

This copy is property of XXX

ACCE CCE Study Guide, v12.0, 2023

Questions
&
Discussions

Ted Cohen, MS, CCE, FACCE
tedcohen@pacbell.net

Please complete the evaluation form for session#8 at: https://www.surveymonkey.com/r/2023-session8

or scan the QR code: