Safeguarding Health Information

Building Assurance through HIPAA Security

SEPTEMBER 3, 2015

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

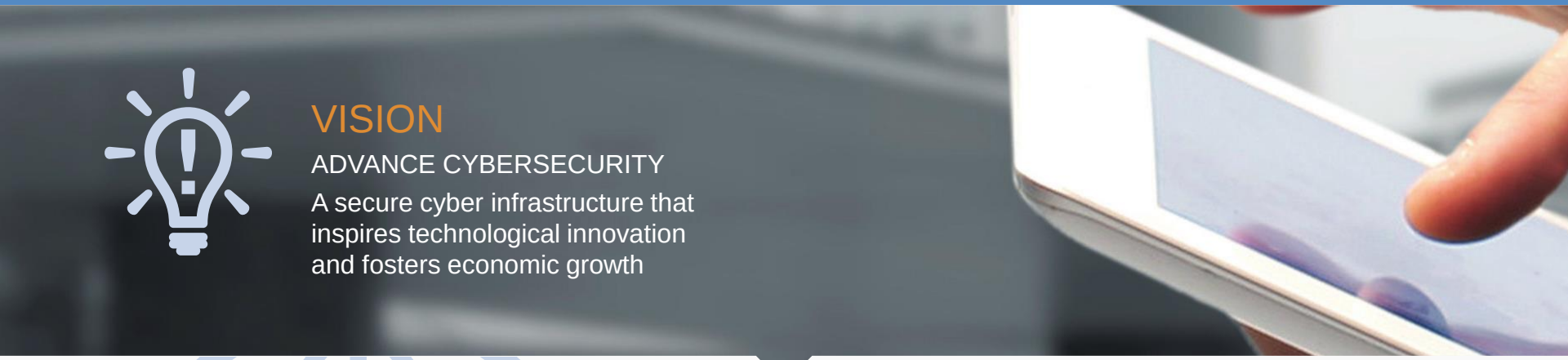
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- NCCoE 101
- EHR and Mobile Device Project
  - Practice Guide
- Wireless Infusion Pumps Project

NCCoE 101

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

VISION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership

GOAL 3

ACCELERATE EFFECTIVE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art collaborative environment

NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

PARTNERSHIPS

The NCCoE is motivated by results. Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.

ITL THOUGHT LEADERSHIP

- Cryptography
- Identity Management
- Key Management
- Risk Management
- Secure Virtualization
- Software Assurance
- Security Automation
- Security for Cloud and Mobility
- Trusted Roots of Hardware
- Vulnerability Management
- Secure Networking
- Usability and Security

STAKEHOLDERS

SPONSORS

Advise, assist, and facilitate the Center's strategic initiatives

- The White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- Maryland State

TEAM

Collaborate with innovators to provide real-world cybersecurity capabilities that address business needs

- NCCoE
- Tech Firms
- Industry
- Academia
- Government
- Project Specialists
- Project-Specific Collaborators
- National Cybersecurity Excellence Partnership (NCEP) Partners

CUSTOMERS

Collaborate with center on project-specific use cases that help our customer's manage their cybersecurity priorities

- Business Sectors
- Individuals
- Academia
- Government
- Cybersecurity IT community
- Systems Integrators

PARTICIPATION BENEFITS

Advance your organization's adoption
of practical cybersecurity solutions that are usable, repeatable and secure

Access integrated cybersecurity solutions
that match your industry's specific business needs

Rely on cybersecurity solutions
that are built on commercially available technologies

Increase your organization's ability to innovate
by bridging technology gaps

Work with cyber innovators
in a trusted, state-of-the-art, collaborative environment

Deepen your organization's understanding
of cybersecurity capabilities, relevant costs and integration and adoption methods

Broaden your organization's awareness
of cybersecurity technologies and standard

NCEP PARTNERS

The NCCoE seeks problems that are

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Two kinds of reference designs

- Sector-specific **use cases** that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific **building blocks** that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

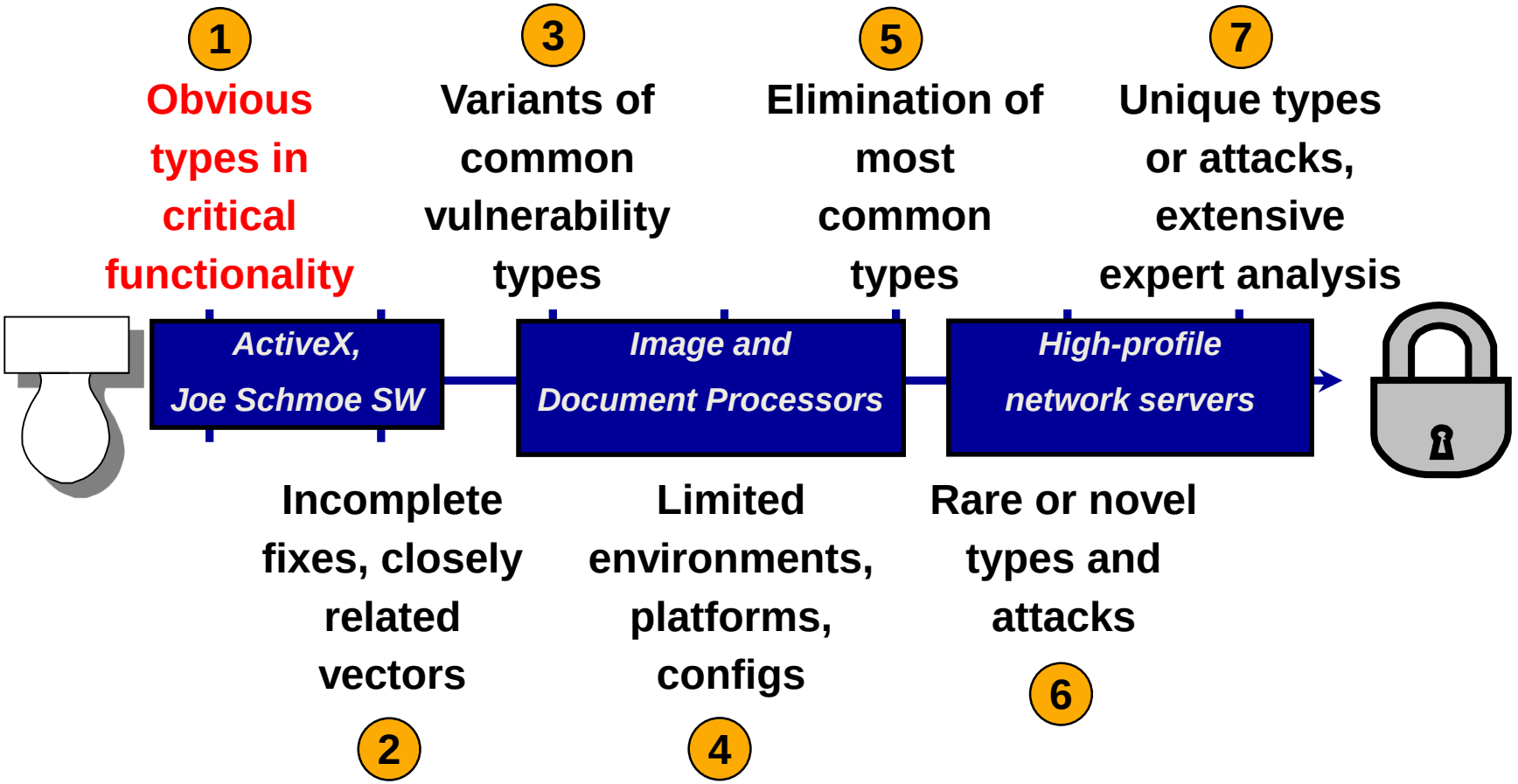
CURRENT SECTORS OF FOCUS

- HEALTH IT
  - EHR and Medical Devices
  - Wireless infusion Pumps
- Energy
- Financial
- Transportation
- Retail

.

Add a health IT sector image…

Resolving healthcare vulnerabilities is in Stage 1



EHR and Mobile Device Project

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

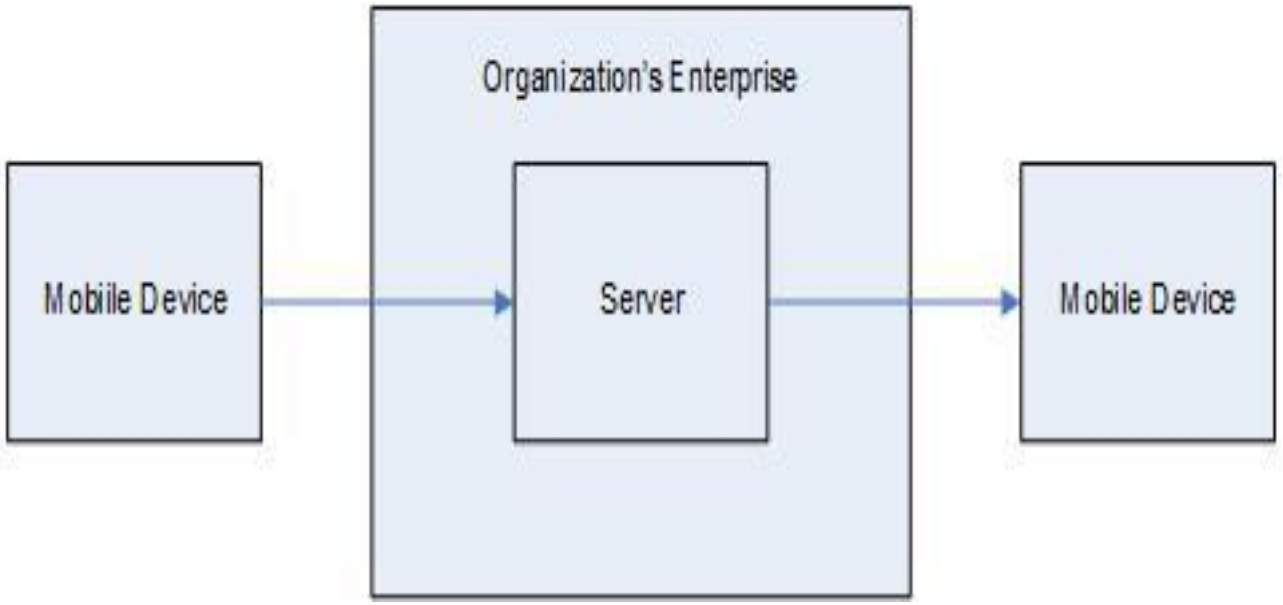
1. Project Plan
2. Use Case
3. Practice Guide
    1. Security Characteristics
    2. Risk Assessment
    3. Control Mappings
    4. Architecture
    5. Evaluation
    6. How-To

Opportunities to participate

1. Outreach to Community of Interest (CoI)
2. Use Case Definition
3. Use Case Definition with Feedback
4. Publish FRN
5. Solicit Letter of Interest
6. Host Vendor Day
7. Sign CRADAs
8. Finalize Roster of Collaborators
9. Develop Draft Architecture Design & Build Plan
10. Create Build
11. Develop Practice Guide
12. Demonstration

1. Physician uses a mobile device application to send a referral to another physician.
2. Application sends the referral to a server running a certified EHR application.
3. Server routes the referral to the referred physician.
4. Referred physician uses mobile device to receive the referral.

.



1. Security of the device itself
2. Security of the data
3. Wireless device data transmission
4. EHR message authentication
5. EHR Network security
6. EHR System Security


CISCO


MEDTECH ENGINUITY CORP.
MEDTEC
"WHERE MEDICAL ENGINEERING & INGENUITY MEET"
© 2011 MedTech Enginuity Corp.


RAMPARTS


RSA


intel


MaaS360
by Fiberlink


Symantec

EHR and Mobile Device Practice Guide

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The guide:

1. Maps security characteristics to standards and best practices from NIST and other standards organizations, and to HIPAA rules
2. Provides a detailed architecture and capabilities that address security controls
3. Facilitates ease of use through automated configuration of security controls
4. Addresses the need for different types of implementation, whether in-house or outsourced
5. Provides a how-to for implementers and security engineers

Methodology Steps

Identify

- thread source and events
- vulnerabilities and predisposing conditions

Determine

- likelihood of occurrence
- determine magnitude of impact
- risk

We offer two methods for conducting risk assessment:

1) Table-driven method
2) Attack/fault-tree assessment methodology

Our risk assessments focused on threats that may lead to the loss of:

- confidentiality – unauthorized disclosure of sensitive information
- integrity – unintended or unauthorized modification of data or system functionality
- availability – impact to system functionality and operational effectiveness

Based on our risk assessment, the major threats to confidentiality, integrity, and availability are:

- a lost or stolen mobile device
- a user
  - walks away from logged-on mobile device
  - downloads viruses or other malware
  - uses an unsecure Wi-Fi network
- inadequate
  - access control and/or enforcement
  - change management
  - configuration management
  - data retention, backup and recovery

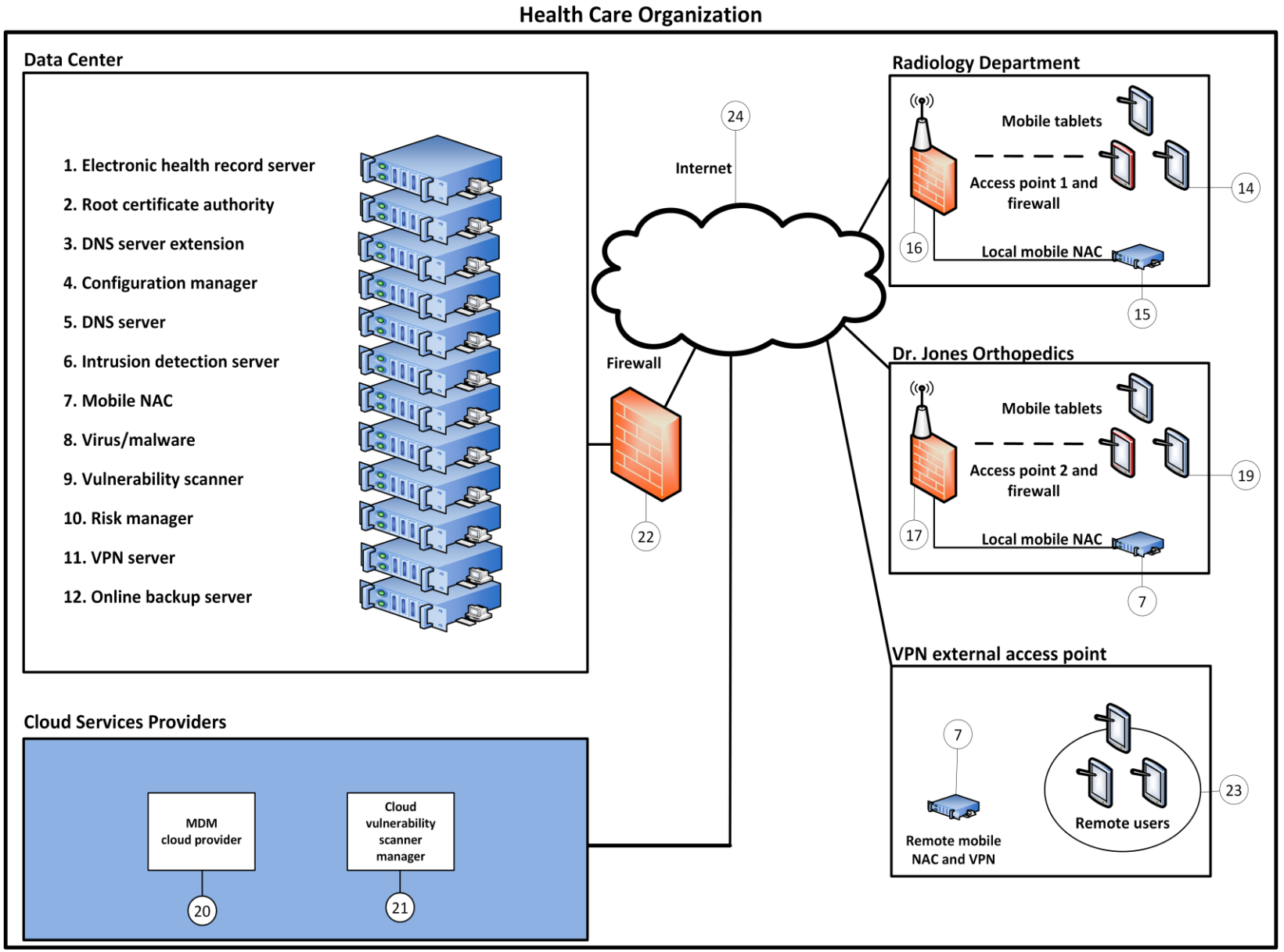
MAPPING CSF FUNCTIONS TO COLLABORATOR PRODUCTS

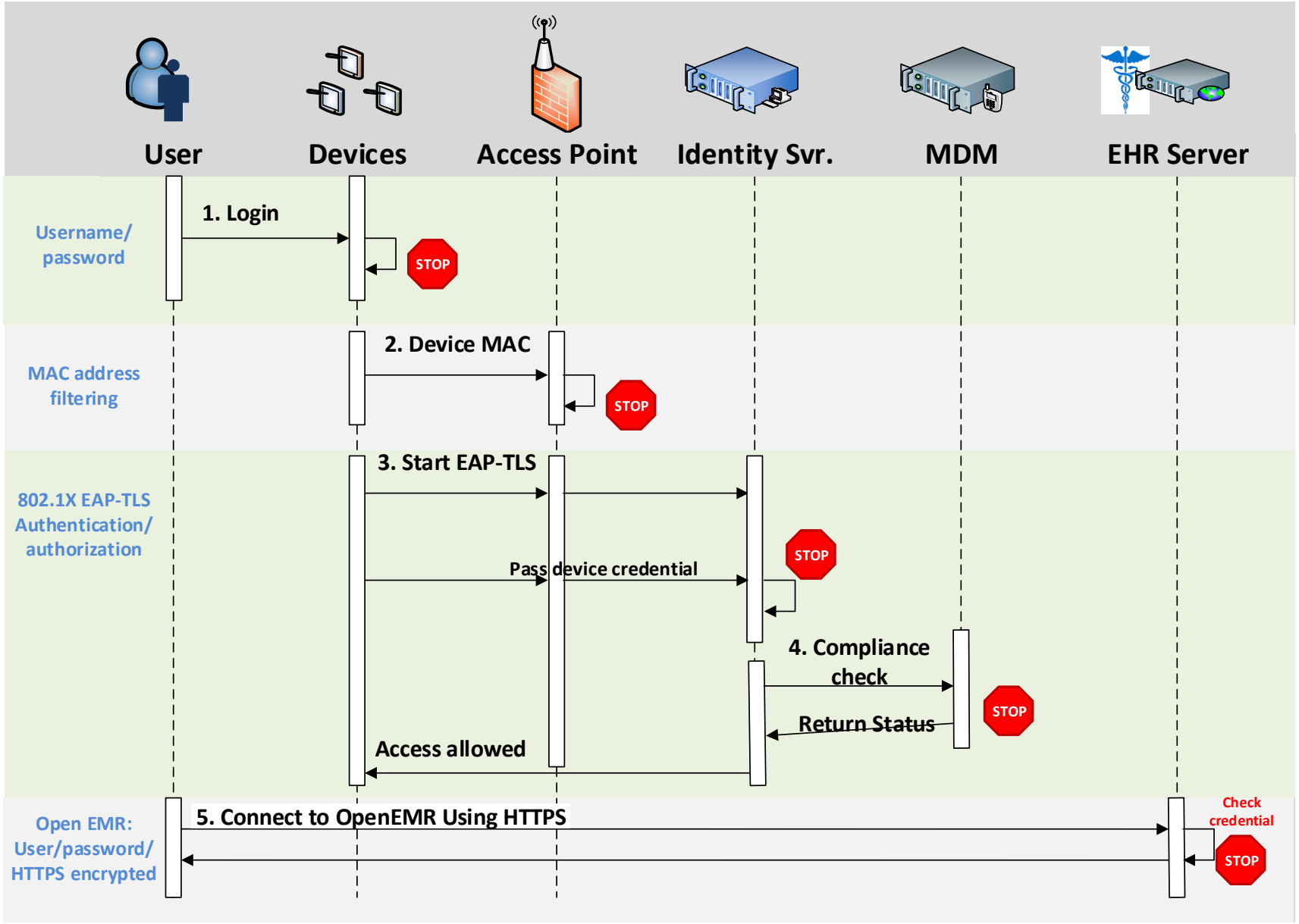
CSF Function	Company	Application / Product	Use
Identify (ID)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	web-based and open source electronic health record and supporting technologies
	open source	Apache Web Server	
	open source	PHP	
	open source	MySQL	
	open source	ModSecurity	Apache module extension, web application firewall (supporting OpenEMR)
	open source	OpenSSL	cryptographically secures transmissions between mobile devices and the OpenEMR web portal service
	Various	mobile devices	Windows, IOS and Android tablets
	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	Root CA / Fedora PKI manager	cryptographically signs identity certificates to prove authenticity of users and devices
	open source	domain name system (DNS) and DNS encryption (DNSE) / Bind9	performs host or fully qualified domain resolution to IP addresses
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	local and remote mobile NAC (Identity Services Engine)	radius-based authentication, authorization and accounting management server
	Cisco	VPN server (ASAv 9.4)	enterprise class virtual private network server based on both TLS and IPSEC
	open source	URbackup	online remote backup system used to provide disaster recovery
	Cisco	wireless access point (RV220W)	Wi-Fi access point

MAPPING SECURITY CHARACTERISTICS TO THE CSF AND HIPAA

Security Characteristics	CSF Function	CSF Category	HIPAA Requirements
access control	Protect (PR)	Access Control (PR.AC)	§ 164.312 (a)
audit controls/ monitoring	Detect (DE)	Security Continuous Monitoring (DE.CM)	§164.312(b)
device integrity	Protect (PR)	Access Control (PR.AC)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Data Security (PR.DS)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Information Protection Processes and Procedures (PR.IP)	(§ 164.312 (c))
		Protective Technology (PR.PT)	(§ 164.312 (c))
	Detect (DE)	Security Continuous Monitoring (DE.CM)	(§ 164.312 (c))
			(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
person or entity authentication	Protect (PR)	Access Control (PR.AC)	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
transmission security	Protect (PR)	Access Control (PR.AC)	§164.312 (e)
		Data Security (PR.DS)	§ 164.312 (e))
		Technology (PR.PT)	§ 164.312 (e))

1. Defense in Depth
2. Modular networks and Systems
3. Traditional Engineering Practices


Health Care Organization
Data Center
1. Electronic health record server
2. Root certificate authority
3. DNS server extension
4. Configuration manager
5. DNS server
6. Intrusion detection server
7. Mobile NAC
8. Virus/malware
9. Vulnerability scanner
10. Risk manager
11. VPN server
12. Online backup server
24
Internet
Firewall
22
Radiology Department
Mobile tablets
Access point 1 and firewall
14
16
Local mobile NAC
15
Dr. Jones Orthopedics
Mobile tablets
Access point 2 and firewall
19
17
Local mobile NAC
7
VPN external access point
7
Remote mobile NAC and VPN
Remote users
23
Cloud Services Providers
MDM cloud provider
20
Cloud vulnerability scanner manager
21


User
Devices
Access Point
Identity Svr.
MDM
EHR Server
Username/ password
1. Login
STOP
MAC address filtering
2. Device MAC
STOP
802.1X EAP-TLS Authentication/ authorization
3. Start EAP-TLS
Pass device credential
STOP
4. Compliance check
Return Status
STOP
Access allowed
Open EMR: User/password/ HTTPS encrypted
5. Connect to OpenEMR Using HTTPS
Check credential
STOP

1. Lost Mobile Device Scenario
2. Internal Network Access Scenario
3. OpenEMR Access Scenario
4. Physical Access Scenario

Mobile Devices

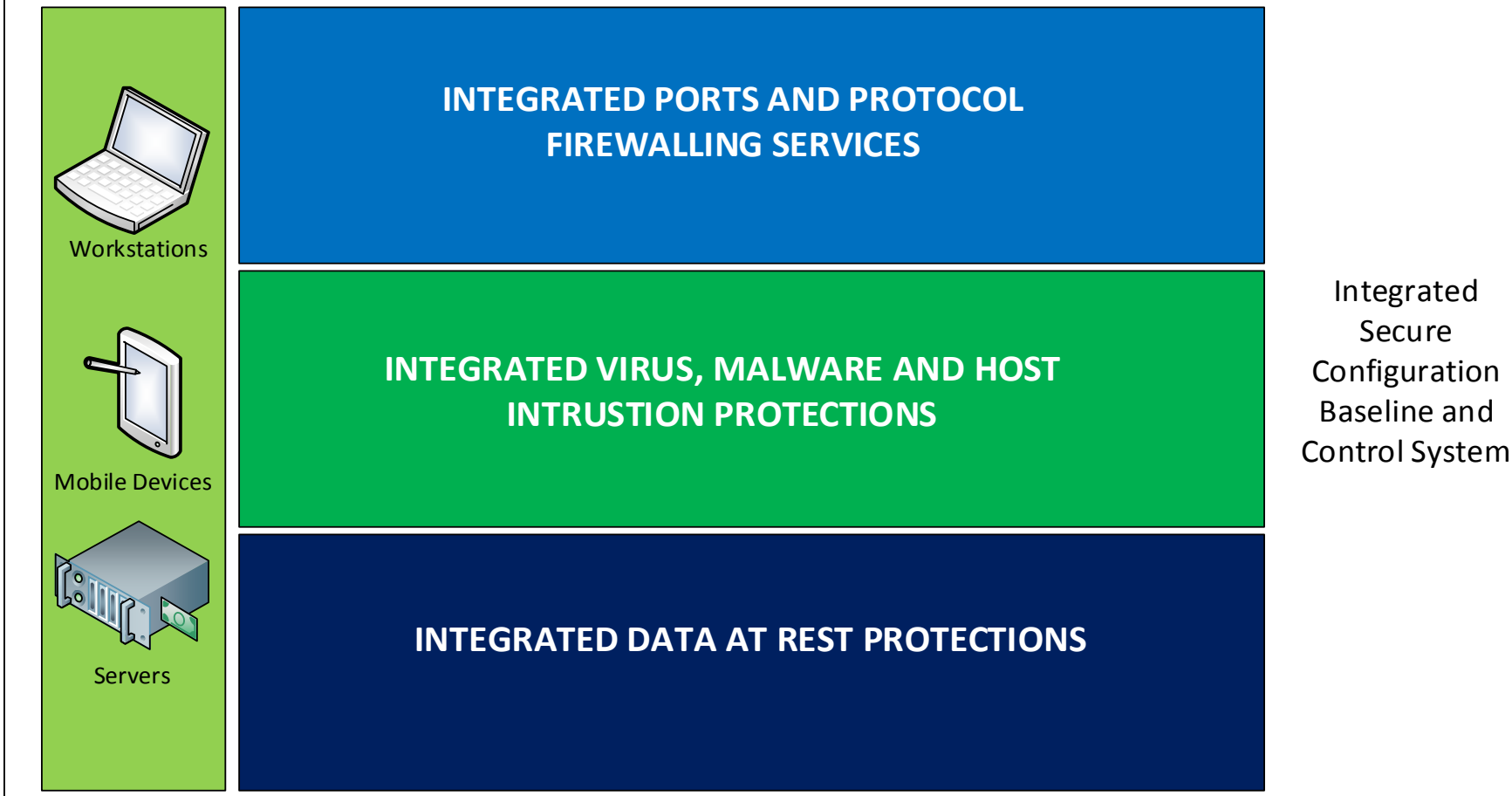
System requirements

•Android device: Android operating system 4.1 and up, screen size 7” and up, and Wi-Fi enabled
•Apple devices: Apple iOS 7 and up, screen size 7” and up, Wi-Fi enabled

You will also need the following parts of this guide:

•Section 3.3, Access Point: Cisco RV220W
•Section 7.1, Fedora PKI
•Section 8.2.1, MDM Setup
•Section 9.1, Cisco Identity Services Engine

Integrated Host Based Security System



Prepare Mobile Device for MDM enrollment

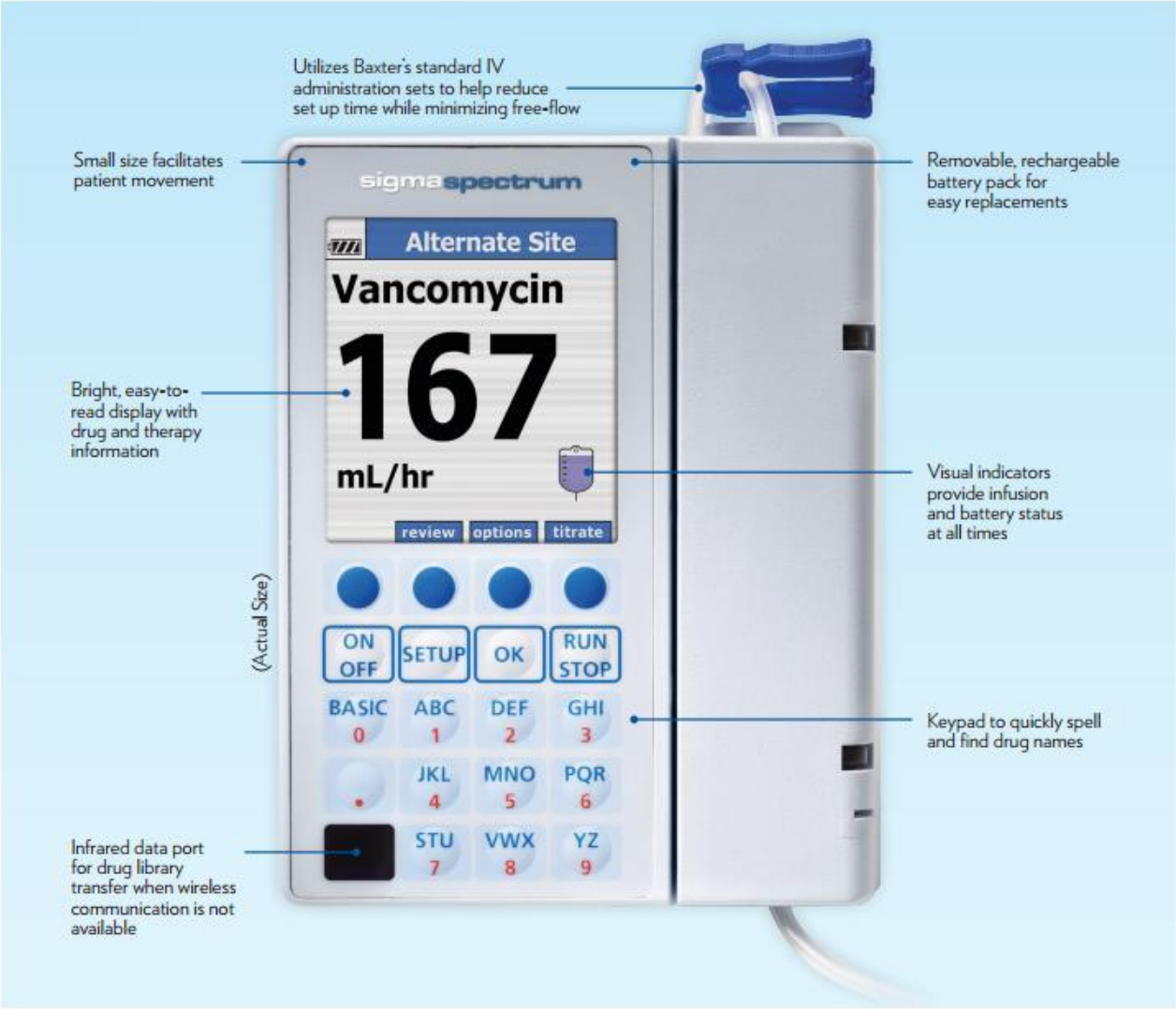
1. Perform factory reset - This step is optional. If factory reset is necessary for an Android device, be sure to check the options for backing up and restoring your data (*https://support.google.com/android-one/answer/2819582*). Follow these steps to perform the factory reset:

- On your mobile device, open the Settings menu.
- Under Personal, tap on Backup & Reset.
- Under Personal data, tap on Factory Data Reset.
- After pressing Reset Device, the device will start to reboot into recovery mode and begin to wipe the tablet and return the device to its factory conditions.
- Startup the device and follow the instructions on the screen to set up the device for a new user. Be sure the Date and Time setting is correct. Otherwise, the wrong date and time could affect the process for validating the certificates for authentication.

Wireless Infusion Pumps Project

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

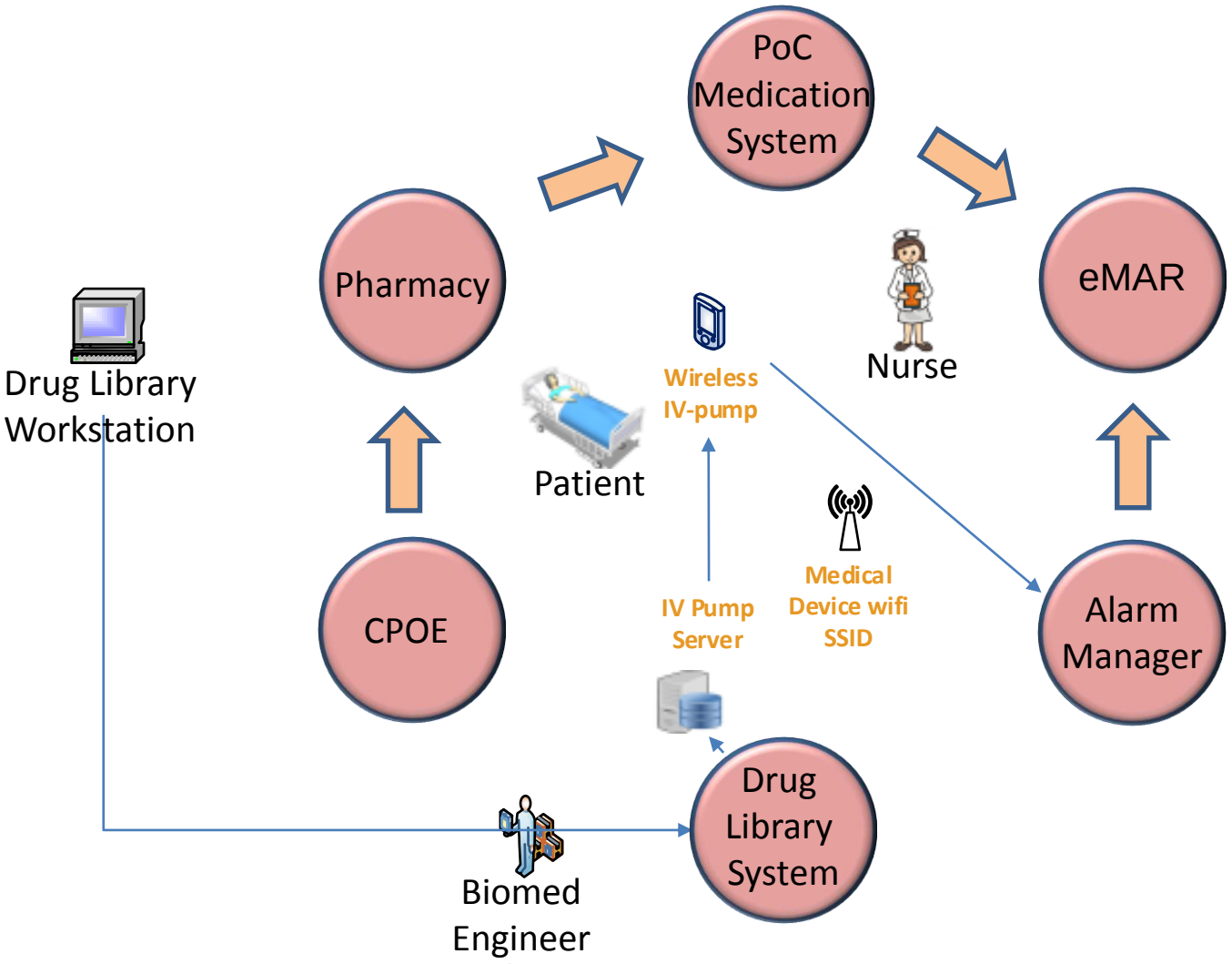

Utilizes Baxter's standard IV administration sets to help reduce set up time while minimizing free-flow
Small size facilitates patient movement
Removable, rechargeable battery pack for easy replacements
Bright, easy-to-read display with drug and therapy information
Visual indicators provide infusion and battery status at all times
Keypad to quickly spell and find drug names
Infrared data port for drug library transfer when wireless communication is not available
(Actual Size)
sigmaspectrum
Alternate Site
Vancomycin
167
mL/hr
review
options
titrate
ON OFF
SETUP
OK
RUN STOP
BASIC 0
ABC 1
DEF 2
GHI 3
JKL 4
MNO 5
PQR 6
STU 7
VWX 8
YZ 9

WIRELESS INFUSION PUMP USE CASE SCOPE

The scope of this use case is to follow the life cycle of an infusion pump from planning the purchase of the pump to decommissioning the device. Life cycle management includes:

- Procurement
- On boarding of asset
- Training and instructions for use
- Configuration
- Usage
- Maintenance
- Decontamination
- Decommissioning Devices

HIGH LEVEL ARCHITECTURE



- The Patient
- The Health Care Professional
- Wireless Infusion Pump
- Pump Server
- Wireless Network
- Alarm Manager
- Electronic Medication Administration Record (eMAR) System
- Point of Care Medication System
- Pharmacy
- Computerized Physician Order Entry (CPOE)
- Drug Library
- Biomed Engineering

INFUSION PUMP SECURITY CHALLENGES

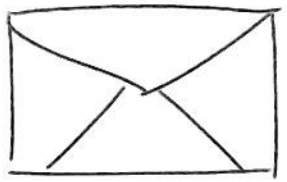
- Access codes
- Access point (AP)/Wireless network configuration
- Alarms
- Asset management and monitoring
- Credentialing
- Credentialing server
- Maintenance and updates
- Pump variability
- Utilization

240-314-6800

hit_nccoe@nist.gov

Participate

http://nccoe.nist.gov



9600 Gudelsky Drive
Rockville, MD 20850