Cybersecurity & the Future of Remote Patient Monitoring

Northern California HIMSS ePatient Summit

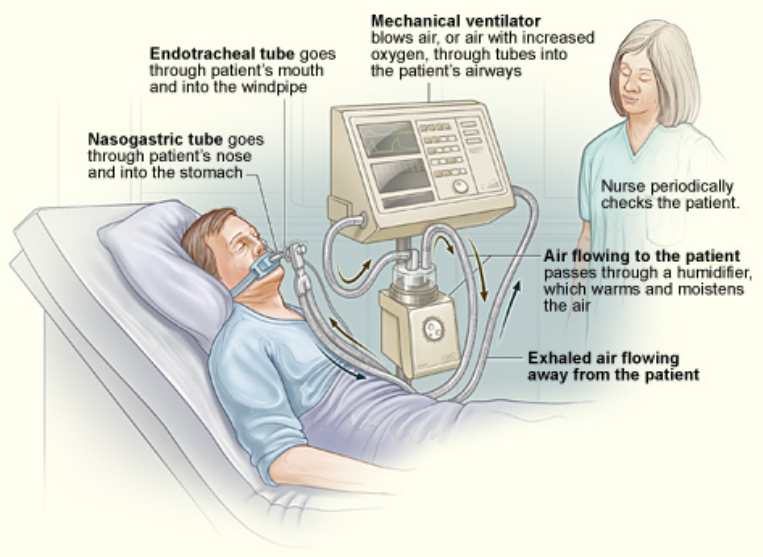
May 12, 2020

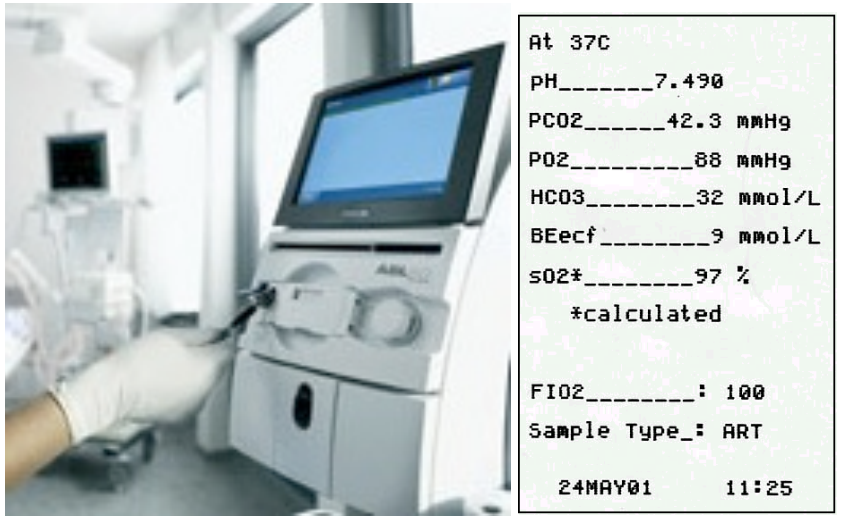
David Snyder, MBA, PE, CISSP, CSM

Four Big Ideas About Remote Patient Monitoring (RPM)

- RPM has been happening for a while & is growing
- Attacks on networks via device vulnerabilities are a bigger concern than attacks on individual devices
- RPM is a **"system of systems"** – not just devices, but devices connected to networks, connected to other networks
- Something that is everybody's responsibility becomes nobody's

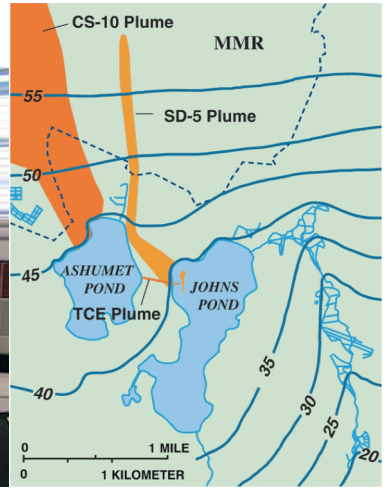
Speaker Background





RESPIRATORY THERAPY

Carnegie Mellon University
Engineering & Public Policy



ENVIRONMENTAL INVESTIGATIONS FIELD & LAB DATA

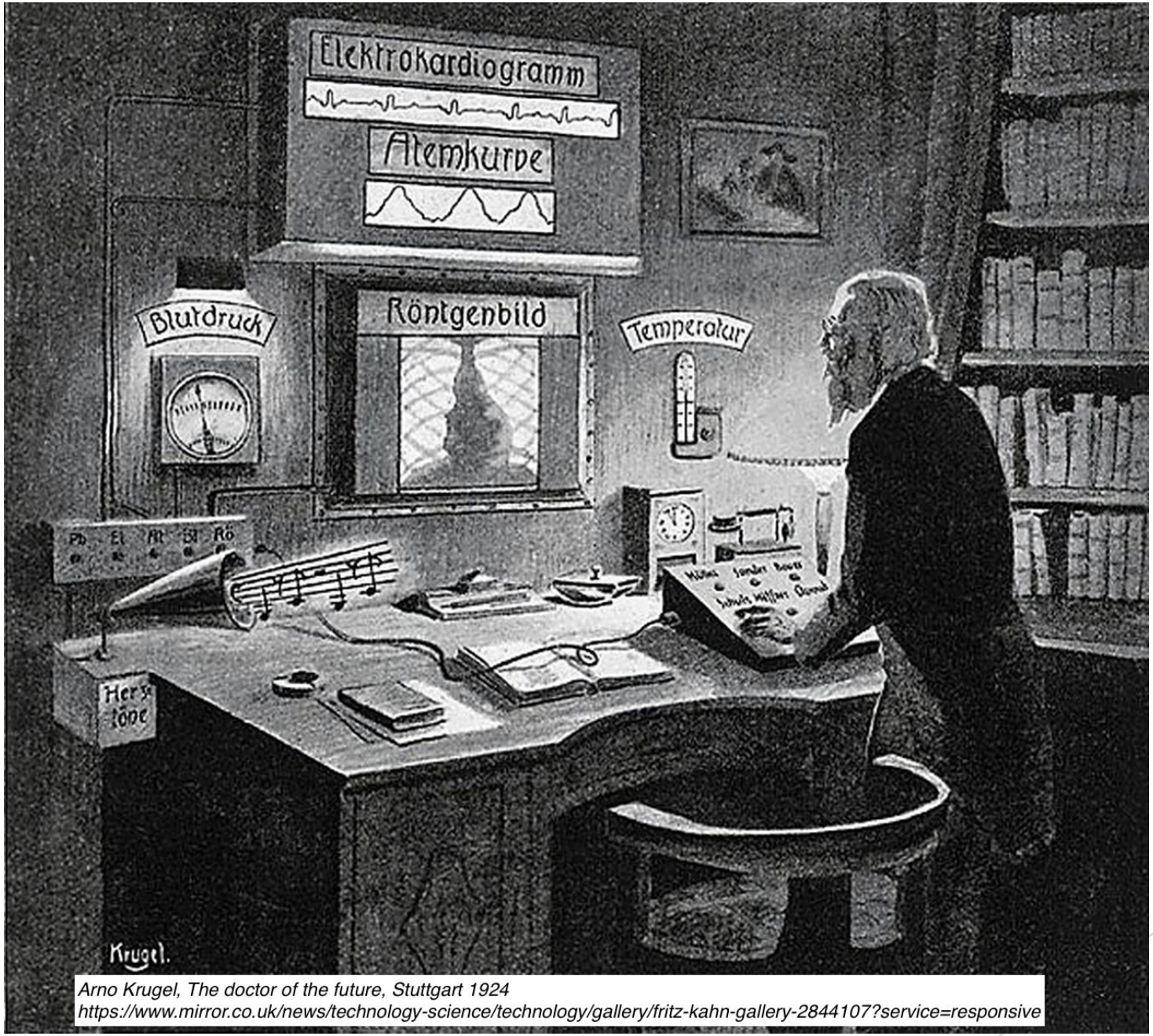
CREDIT CARD SYSTEMS

CISSP®

Certified Information Systems Security Professional

HealthTech Meetup

Remote Patient Monitoring was imagined long ago…



Arno Krugel, The doctor of the future, Stuttgart 1924
https://www.mirror.co.uk/news/technology-science/technology/gallery/fritz-kahn-gallery-2844107?service=responsive

This Presentation

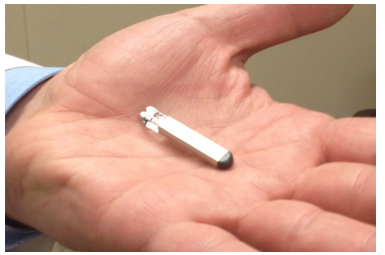
- Introductions & Context
- How RPM Works
- System of Systems / Teamwork
- Vulnerabilities, Threats, and Attacks
- Risk Assessment
- Best Practices
- References

Home Monitoring

Clinician Reviews Results

April 2020 TV News

Common Connected RPM Devices



Healthcare in the US

- Over 6,000 hospitals with over 36 million admissions per year – over 900,000 beds
- Thousands of ambulatory surgery centers, clinics, and doctor offices
- Over 900,000 physicians and over 3 million nurses
- Over $3 Trillion per year = 17.9% of US GDP (and forecast to go up) (over $1 Trillion spent in hospitals)
- Thousands of medical devices in typical hospital
- Increasing use of remote monitoring

Home Health Services

- Number of home health agencies: 12,200 (2016)
- Number of patients who received and ended care any time during the year: 4.5 million (2015)

https://www.cdc.gov/nchs/fastats/home-health-care.htm

…and this does not even consider people living in Independent Living, Assisted Living, and Skilled Nursing Facilities.

Trends

- Aging population
- Chronic illnesses
- Shortage of caregivers & professionals
- Incentives to reduce hospital readmissions
- Telehealth reimbursement codes
- More and more devices
- COVID-19: avoiding office visits is a good way to avoid exposure and spread

Chronic Illness

6 IN 10

Adults in the US have a **chronic disease**

4 IN 10

Adults in the US have **two or more**

THE LEADING CAUSES OF DEATH AND DISABILITY
and Leading Drivers of the Nation's **$3.5 Trillion** in Annual Health Care Costs

Common Conditions & RPM

- Diabetes
- Hypertension (high blood pressure)
- Congestive heart failure
- Arrhythmia, including atrial fibrillation
- Chronic obstructive pulmonary disease (COPD)
- Asthma
- Kidney disease
- Medication adherence

Telehealth Reimbursement Codes

- **CPT code 99453:** "Remote monitoring of physiologic parameter(s) (e.g, weight, blood pressure, pulse oximetry, respiratory flow rate), initial set-up and patient education on use of equipment."
  - What to know: CPT 99453 offers reimbursement for the work associated with onboarding a new patient onto a RPM service, setting up the equipment and educating the patient on using the equipment. The average national Medicare payment for these services is $19.46.
- **CPT code 99454:** "Device(s) supply with daily recording(s) or programmed alert(s) transmission, each 30 days."
  - What to know: CPT 99454 offers reimbursement for providing the patient with a RPM device for a 30-day period. Note that 99454 can be billed each 30 days. The average national Medicare payment for these services is $64.15.

Telehealth Reimbursement Codes (continued)

- **CPT code 99457:** "Remote physiologic monitoring treatment management services, 20 minutes or more of clinical staff/physician/other qualified healthcare professional time in a calendar month requiring interactive communication with the patient/caregiver during the month."
  - What to know: Under this new code, CMS will reimburse for clinical staff time that contributes toward monitoring and interactive communication which includes phone, text and email. The average national Medicare payment for these services is $51.54 (non-facility) and $32.44 (facility).

Telehealth Reimbursement Codes (continued)

- **CPT code 99091:** "Collection and interpretation of physiologic data (e.g. ECG, blood pressure, glucose monitoring) digitally stored and/or transmitted by the patient and/or caregiver to the physician or other qualified healthcare professional, qualified by education, training, licensure/regulation (when applicable) requiring a minimum of 30 minutes of time, each 30 days."
  - What to know: Under this existing code, CMS will reimburse for professional time dedicated to monitoring services and does not require interactive communication like 99457 to bill. However, it requires a physician or other QHP to perform these services, and requires 30 minutes of time every 30 days to bill. 99457 and 99091 cannot be billed concurrently. The average national Medicare payment for these services is $58.38.

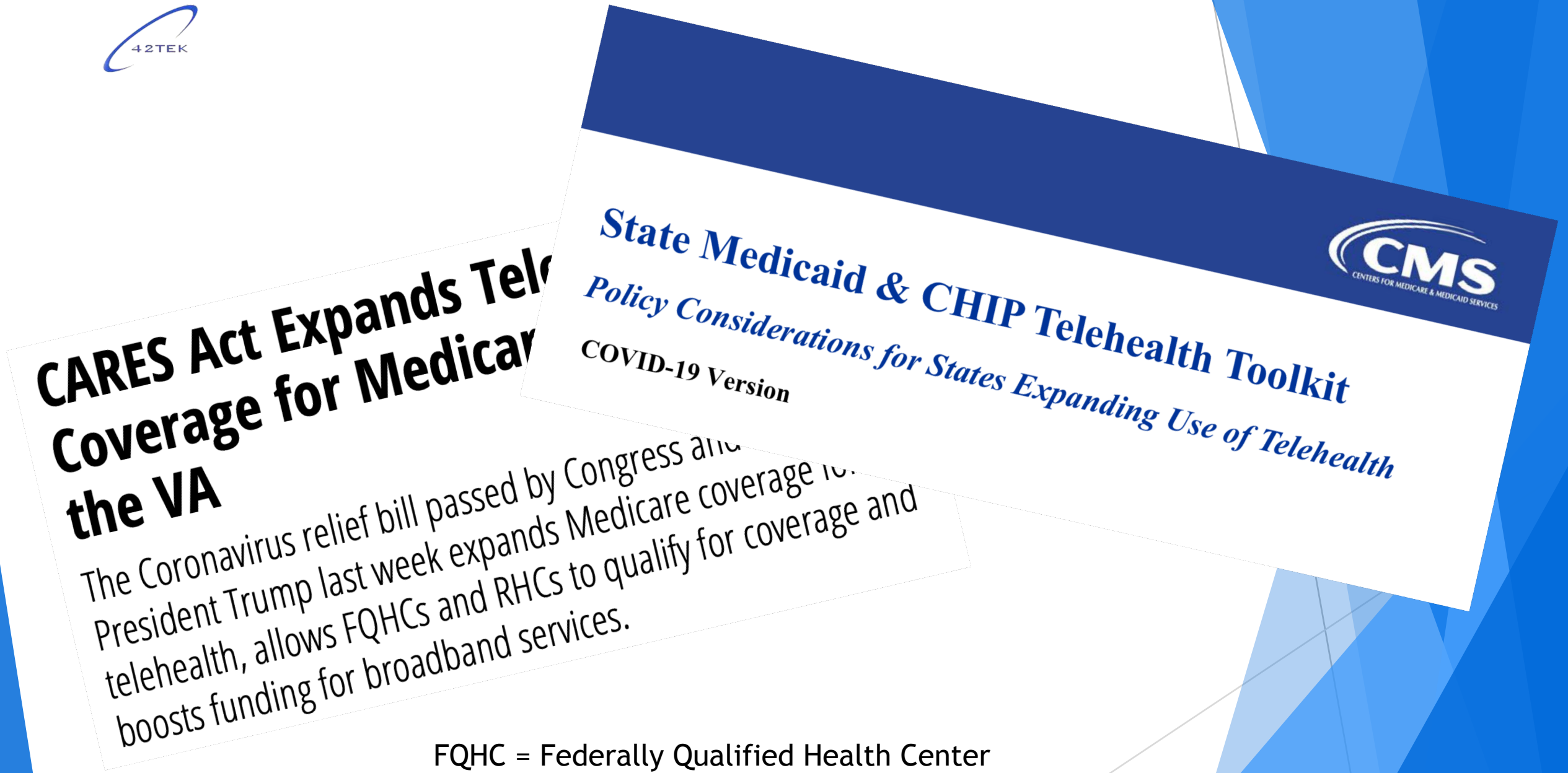
https://www.propellerhealth.com/2019/04/09/your-guide-to-the-new-cpt-codes-for-remote-patient-monitoring/

Telehealth Reimbursement Codes (continued)

- CPT code 99458 (Remote physiologic monitoring treatment management services, clinical staff/physician/other qualified health care professional time in a calendar month requiring interactive communication with the patient/caregiver during the month; additional 20 minutes)

  https://www.getqardio.com/qardiomd-blog/cms-finalizes-2020-cpt-code-rules-remote-patient-monitoring/

- Additional information at https://www.cchpca.org/sites/default/files/2019-11/FINALIZED%20PFS%20CY%202020%20FINAL.pdf



FQHC = Federally Qualified Health Center
RHC = Rural Health Clinic

High Level View

HOW REMOTE MONITORING WORKS

1 SCHEDULE
Clinic schedules dates for the patient to send information from their device to the clinic.

2 SEND
Device information is sent automatically (for wireless ICDs) or manually by the patient (for pacemakers).

3 TRANSMIT
Device information travels from the remote monitor to the clinic.

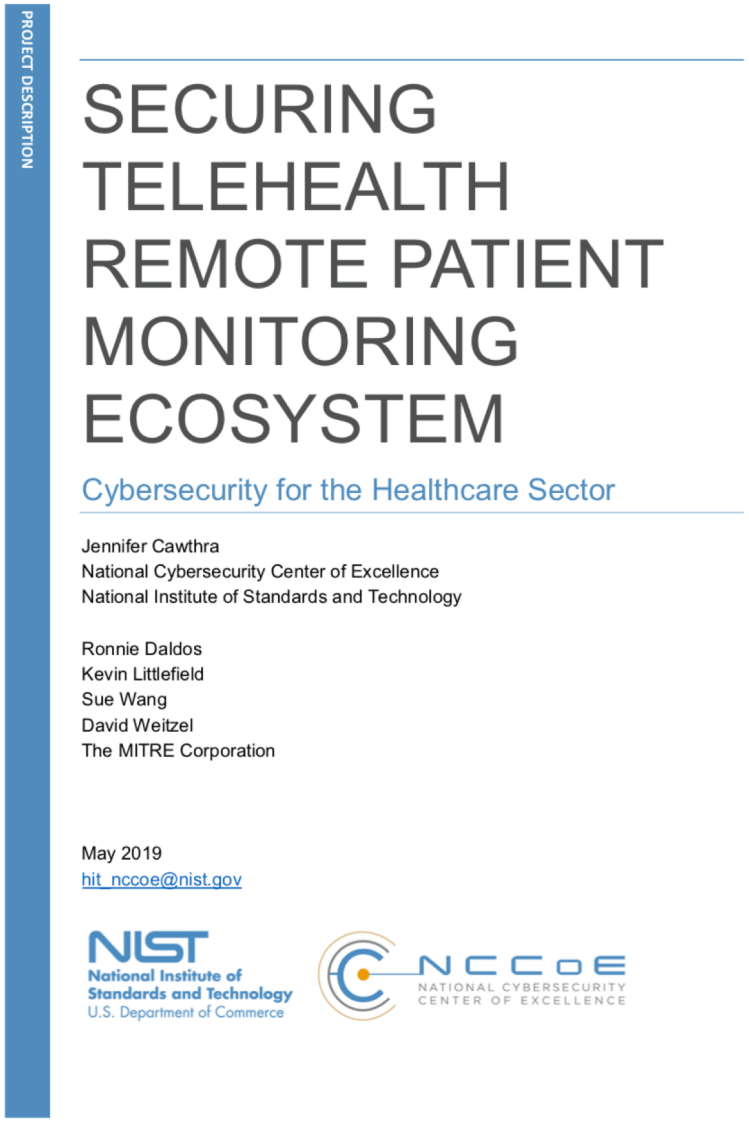
4 REVIEW
The clinic reviews the device information on a secure website.

Remote Monitoring Network: a System of Systems

- Device
- Local communications
- External communications
- Cloud data service (or Healthcare Delivery Organization servers)
- Communication to HDO (or internal HDO network)
- Electronic Medical Record
- Care provider data access device (typically app on PC or mobile device)

- “Glucose meters, ECGs and blood pressure monitors are among the most common types of RPM equipment used, but the array of available technologies is rapidly expanding.”
  - **Remote Patient Monitoring Brings Healthcare To Your Home**, November 27, 2019, Forbes https://www.forbes.com/sites/forbestechcouncil/2019/11/27/remote-patient-monitoring-brings-healthcare-to-your-home/#403eb3e43785
- CPAP machines may also be among the high numbers.

National Institute of Science and Technology


PROJECT DESCRIPTION

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cawthra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Daldos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov

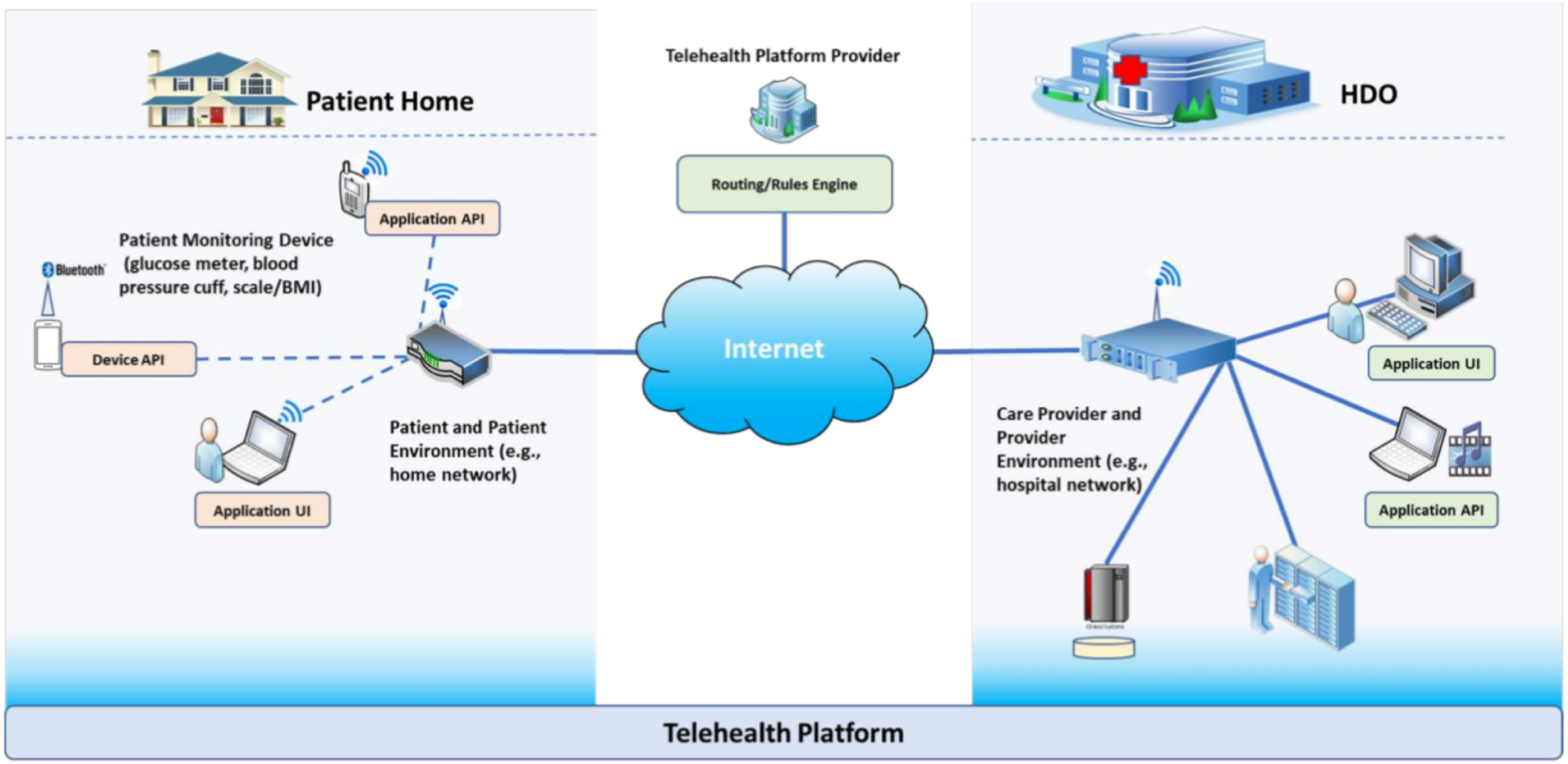
NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

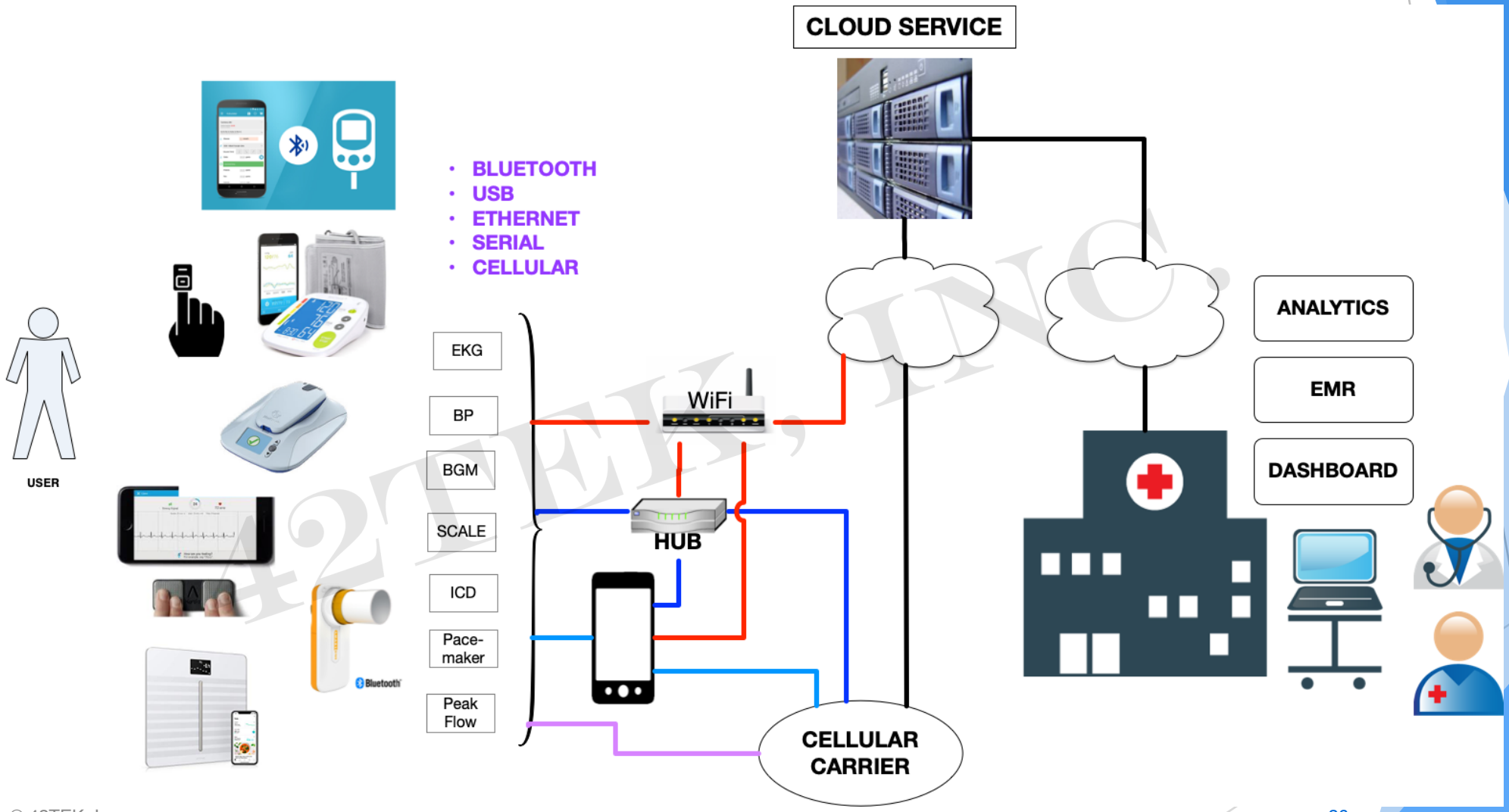
https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-draft.pdf

NIST RPM model

Figure 3-1: High-Level Architecture



Alternate Model



Or land line

Connectivity Option	Hardware	Home Considerations
Internet	LATITUDE Ethernet Adapter or Wireless Internet Adapter	Requires access to high speed Internet modem/router
Cellular	LATITUDE Cellular Adapter	Service provided by AT&T and T-Mobile
Landline	Included with the LATITUDE Communicator	Compatible with most analog and digital phone services

Similarities with In-Hospital Systems

- Patient safety depends on availability when needed
- Patient safety depends on integrity of data (including provenance)
- Personal Health Information or Personally Identifiable Information may be present
- Potential for malicious or unintended network connections
- Need for patching/updating
- Need for authentication, authorization & encryption

Differences

Hospital	Remote Monitoring
Often capital equipment	Expense item
Long useful life	May not have long life
On-site IT & clinical engineers	No on-site support
Logging & monitoring	Logging/monitoring less likely
Network segmentation possible	Typically cloud platform
Many people around	Few people around

“PATIENT TECHNOLOGY

Remote encounters *often involve technology or internet connections that are not provided by the telemedicine organization*. Patient computers, tablets, or smartphones may be used to connect with providers. Telemedicine encounters at the patient’s home are connected through the patient’s home Wi-Fi network where interface issues at the patient location may occur such as lagging video feed, low-quality video, or internet outages.

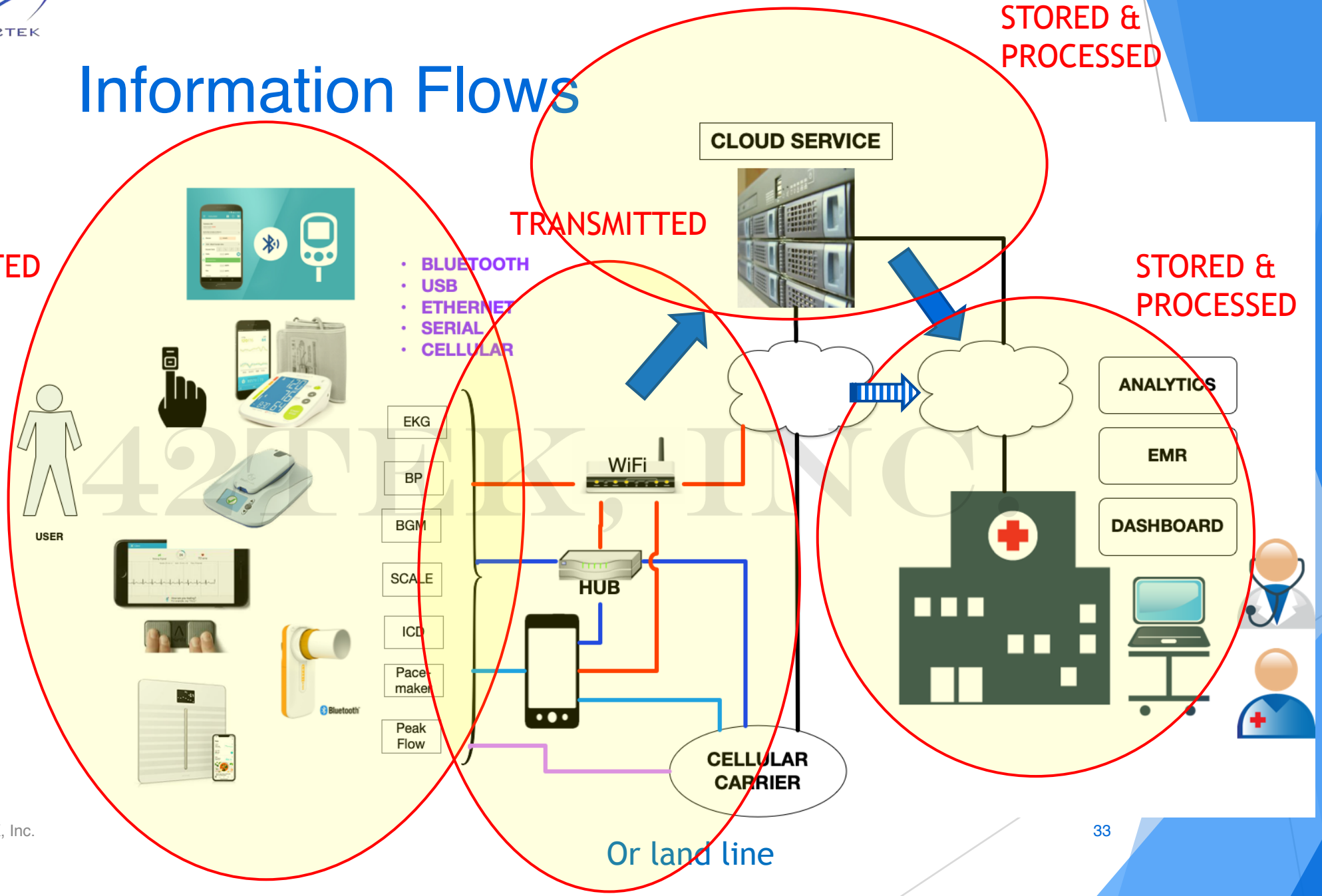
https://healthsectorcouncil.org/wp-content/uploads/2018/08/AHIMA-Telemedicine-Toolkit.pdf

In addition, a patient's home Wi-Fi network or mobile device does not have the same security features as an organization's system. This could potentially risk patient privacy and security. The telemedicine platform and feed must be secure and encrypted during all patient encounters.

For some patient encounters, the technology itself can be a challenge. Some patients may not be as familiar with the functionality of their mobile devices, internet connection, or telemedicine application. It is important that providers remain patient and offer guidance along the way.

Remote Patient Monitoring

Information Flows



Whose Job Is It?

- This is a story about four people named **Everybody**, **Somebody**, **Anybody**, and **Nobody**.
- There was an important job to be done and **Everybody** was asked to do it.
- **Everybody** was sure **Somebody** would do it.
- **Anybody** could have done it, but **Nobody** did it.
- **Somebody** got angry about that, because it was **Everybody's** job.
- **Everybody** thought **Anybody** could do it but **Nobody** realized that **Everybody** wouldn't do it.
- It ended up that **Everybody** blamed **Somebody** when **Nobody** did what **Anybody** could have done.

* apparently an adaptation of “The Responsibility Poem” by Charles Osgood attributed to Charles R. Swindoll

https://www.goodreads.com/quotes/829722-this-is-a-story-about-four-people-named-everybody-somebody

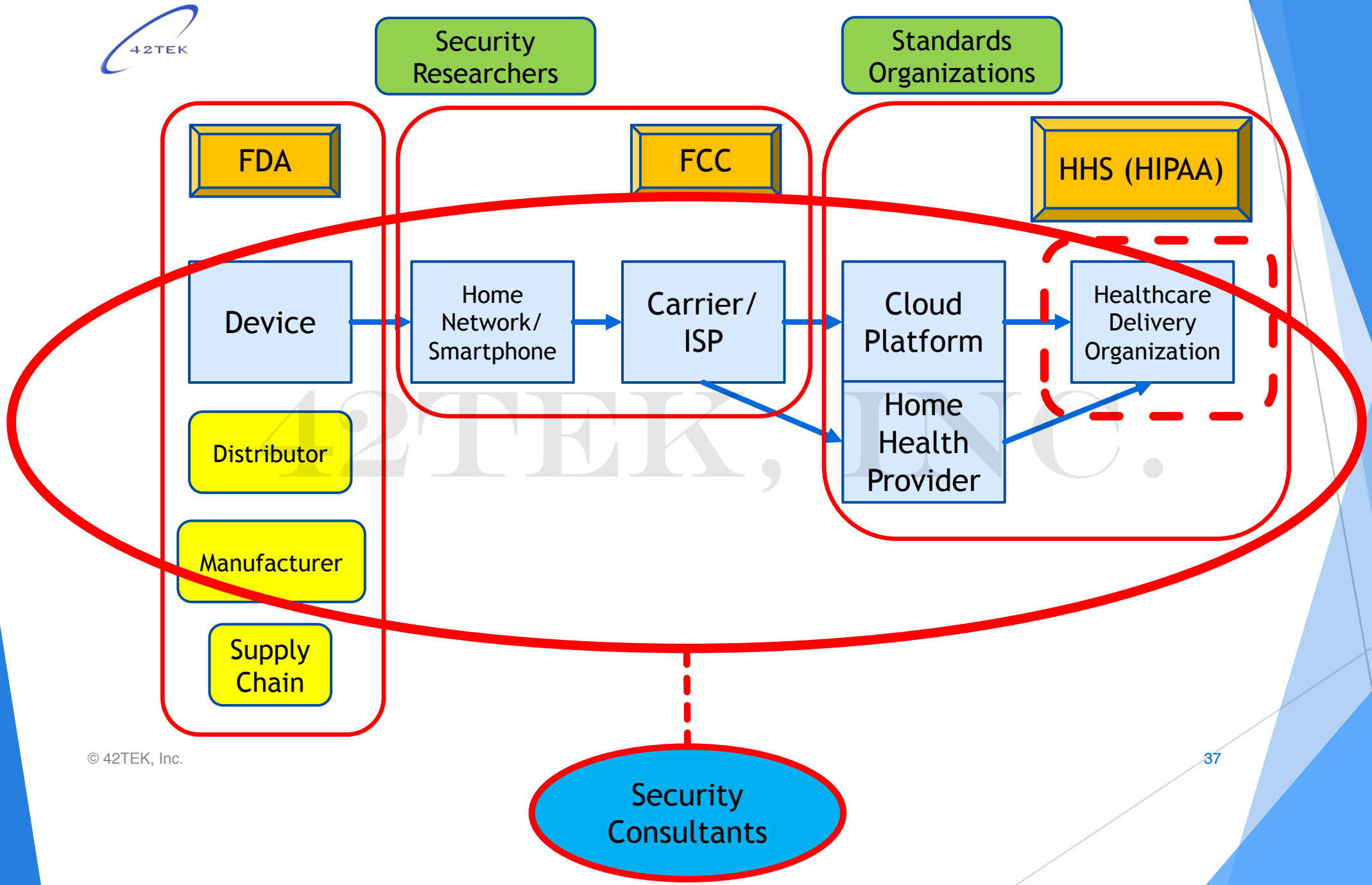
Who is Everybody?

- End user (patient; home health care provider)
- Device manufacturer
- Network equipment manufacturer
- Communications equipment manufacturer
- Telecommunications carrier
- Internet Service Provider
- Cloud platform service provider
- Healthcare Delivery Organization IT staff
- Healthcare Delivery Organization clinical engineers
- Clinical staff
- Food & Drug Administration
- Federal Communications Commission
- Standards organizations

FDA Post-Market Guidance

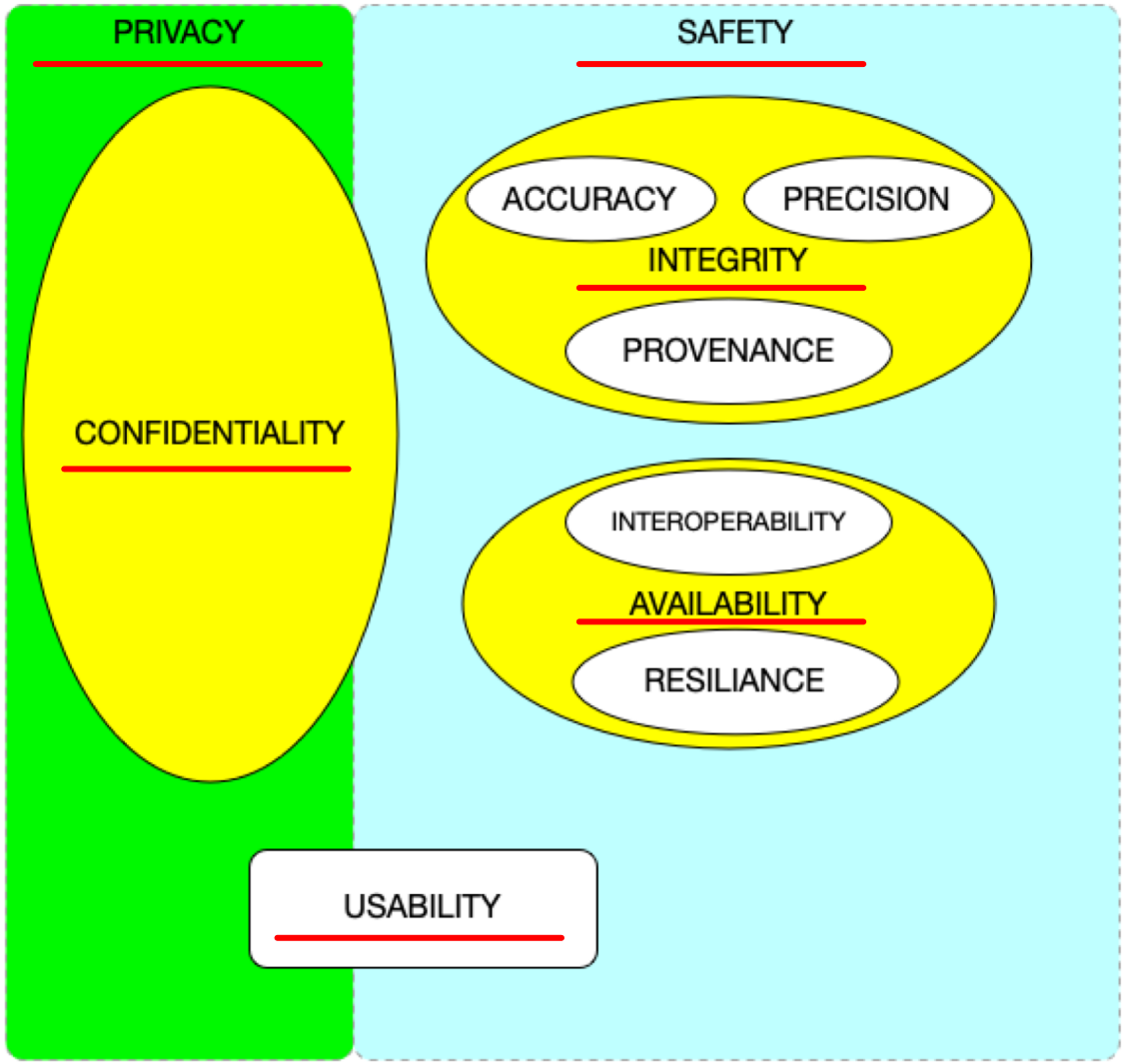
- "Cybersecurity risk management is a shared responsibility among stakeholders including the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA. FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it regulates, recommendations associated with mitigating cybersecurity threats to device functionality and device users."

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

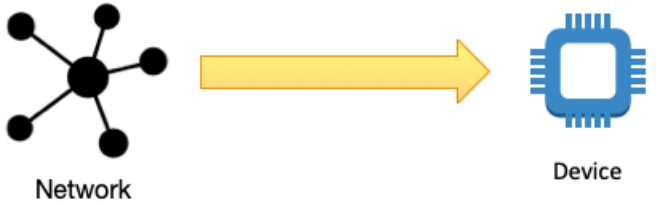

Security Researchers
Standards Organizations
FDA
FCC
HHS (HIPAA)
Device
Home Network/ Smartphone
Carrier/ ISP
Cloud Platform
Healthcare Delivery Organization
Distributor
Home Health Provider
Manufacturer
Supply Chain
Security Consultants

Cybersecurity Concepts & Best Practices

Confidentiality, Integrity, Availability

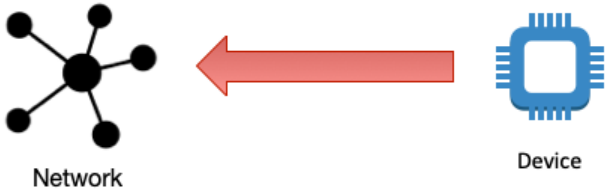


Connected Device Security



- Medical devices can be targets for attack from elsewhere on the network

- Medical devices can be a entry point for gaining entry to hospital network



Cybersecurity is Not Just About Attacks

It's also about compatibility and interoperability

TECHNOLOGY CORONAVIRUS PANDEMIC

COVIDSafe may interfere with diabetes-monitoring apps

For our free coronavirus pandemic coverage, learn more here.

By **Tim Biggs**
May 1, 2020 — 1.08pm

The government's new COVIDSafe contact tracing app may interfere with Bluetooth-connected medical devices such as those used by people with diabetes.

https://www.smh.com.au/technology/covidsafe-may-interfere-with-diabetes-monitoring-apps-20200501-p54oyd.html

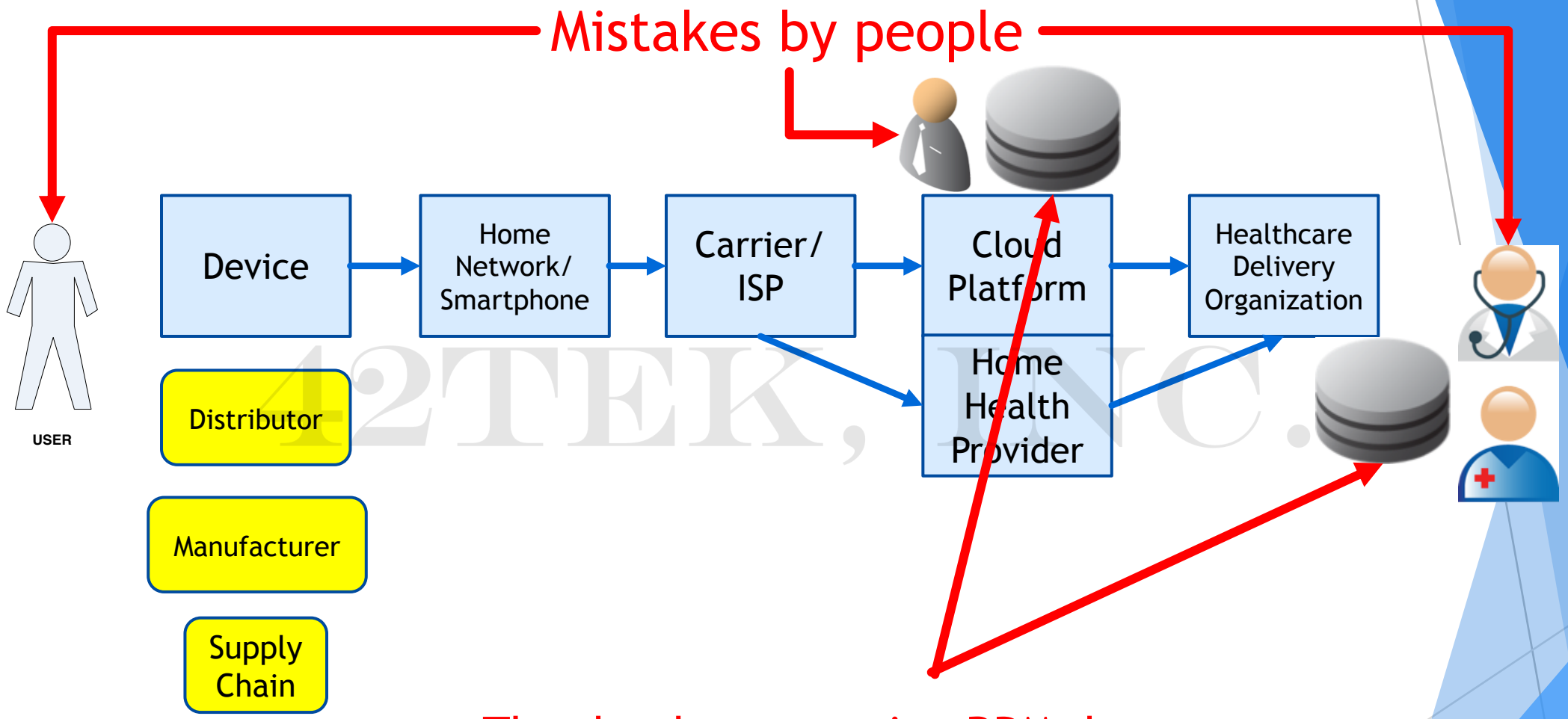
- VULNERABILITY - a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- THREAT - a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- EXPLOIT - an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat

Unlocked door

Burglar, Hacker, Malware or "Bot" or Interference

- VULNERABILITY - a weakness which allows an [illegible] reduce a system's information assurance [illegible]erability is the intersection of three elements: a [illegible]m susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- THREAT - a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- EXPLOIT - an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat

Break-in; Vandalism



The databases storing RPM data

Top Vulnerabilities for RPM

- Out-of-date operating systems or software
- Unpatched systems (both monitoring devices and network components)
- Inadequate network segmentation
- Default or weak passwords
- Misconfiguration
- Poor identity and access management
- Third party network connections
- Poor physical security (allowing tampering with devices)
- Lack of logging and monitoring
- Lack of intrusion detection

Top Threats for RPM

- Denial of service
- Social engineering (incl. phishing)
- Ransomware
- Tampering
- Man-in-the-Middle
- Advanced persistent threats (sophisticated attackers, like nation-states)

Reported Vulnerabilities

- “URGENT/11: FDA issues alert for cyber vulnerability that threatens medical devices, networks”
- “FDA Issues Safety Alert on Cybersecurity Vulnerabilities of Medtronic ICD, CRT Devices”
- “Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers”
- “J&J warns diabetic patients: Insulin pump vulnerable to hacking”
- “FDA Warns of Cybersecurity Vulnerabilities in CareLink Programmers”

The FDA is “not aware” of any instances where a patient has been harmed due to a cybersecurity incident.

“A recent anonymous international study from the University of California Cyber Team funded by MedCrypt found that a few healthcare delivery organizations and vendors believe between 100 and 1,000 patients had adverse events from compromised healthcare infrastructure cybersecurity events, like ransomware, malware, compromised EHRs or an attack on facility systems.”

https://www.healthcareitnews.com/news/security-risk-storm-here-medical-device-threats-are-real-and-patient-safety-risk

Typically, we just don’t have good ways to know whether something bad has happened…

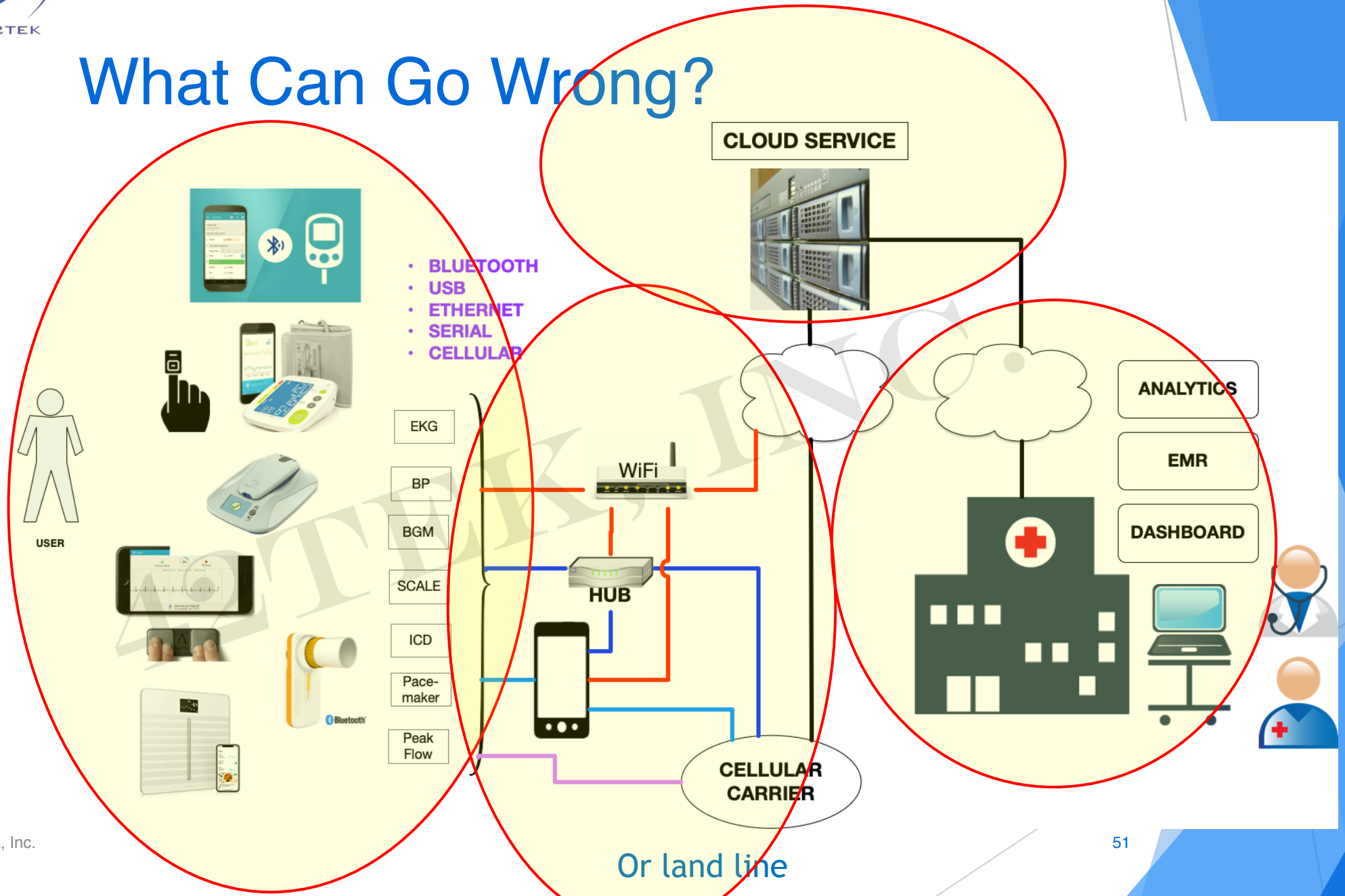
This is part of a larger issue with medical errors and reporting

"To work in this field, you have to become devious yourself. You have to think like a malicious attacker to find weaknesses in your own work…"

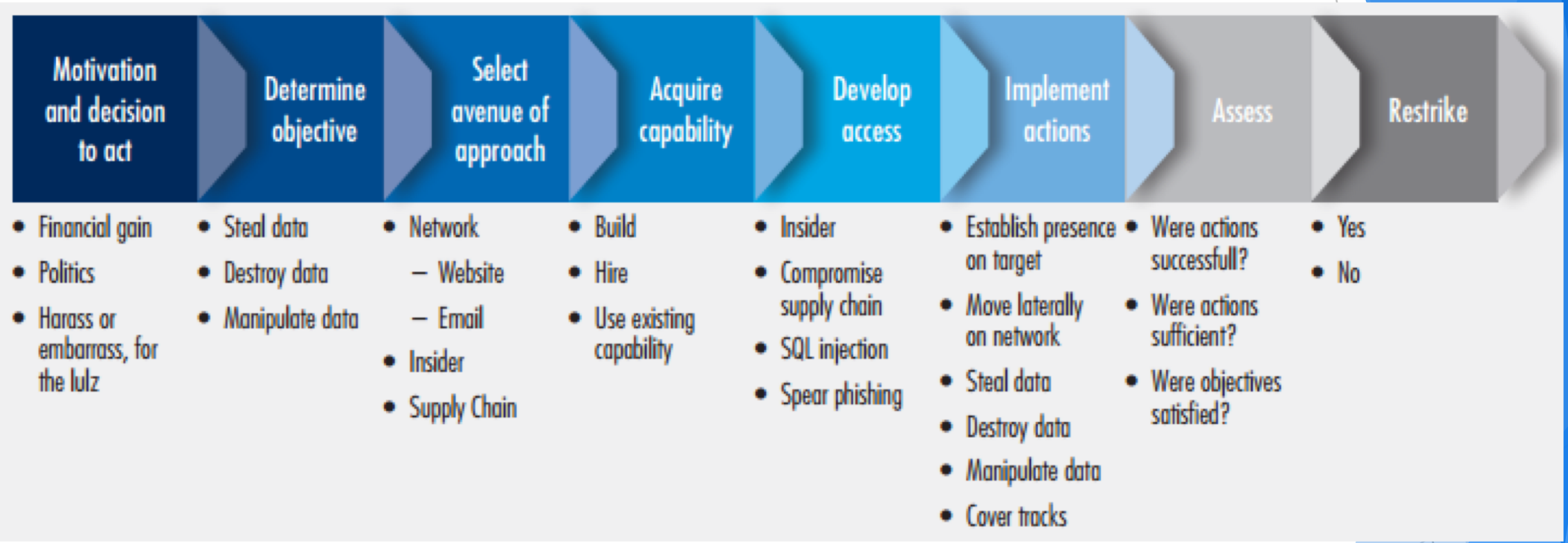
-- Cryptography Engineering

Ferguson, Schneier, & Kohno, 2010

What Can Go Wrong?



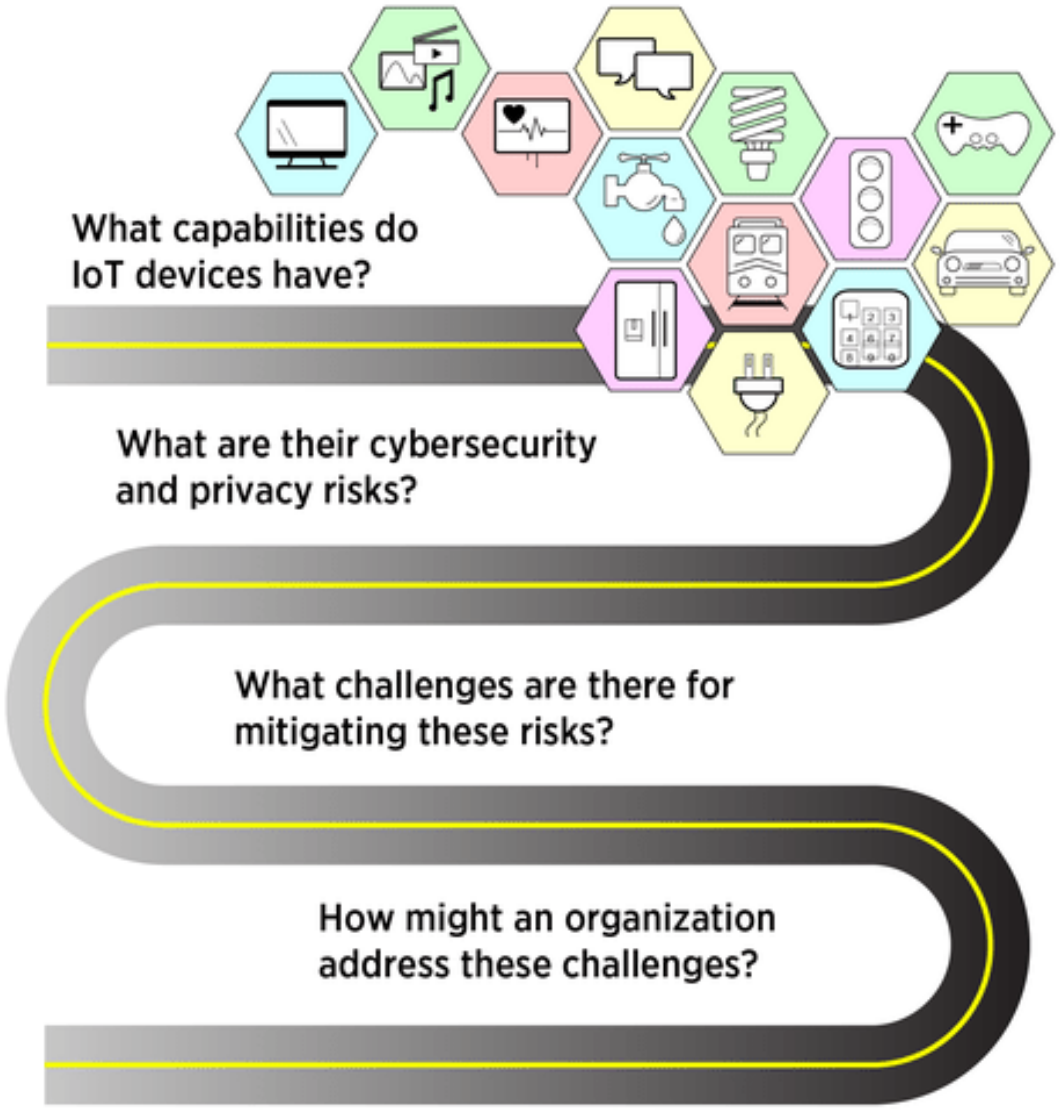
Attack “Kill Chain”



Common Attacks

- Phishing to steal usernames and passwords to get into networks
- Denial of Service – disrupting network
- Ransomware – encryption of data
- Exploiting a vulnerability on one piece of equipment on the network to “pivot” to other parts of the network

Risk Assessment

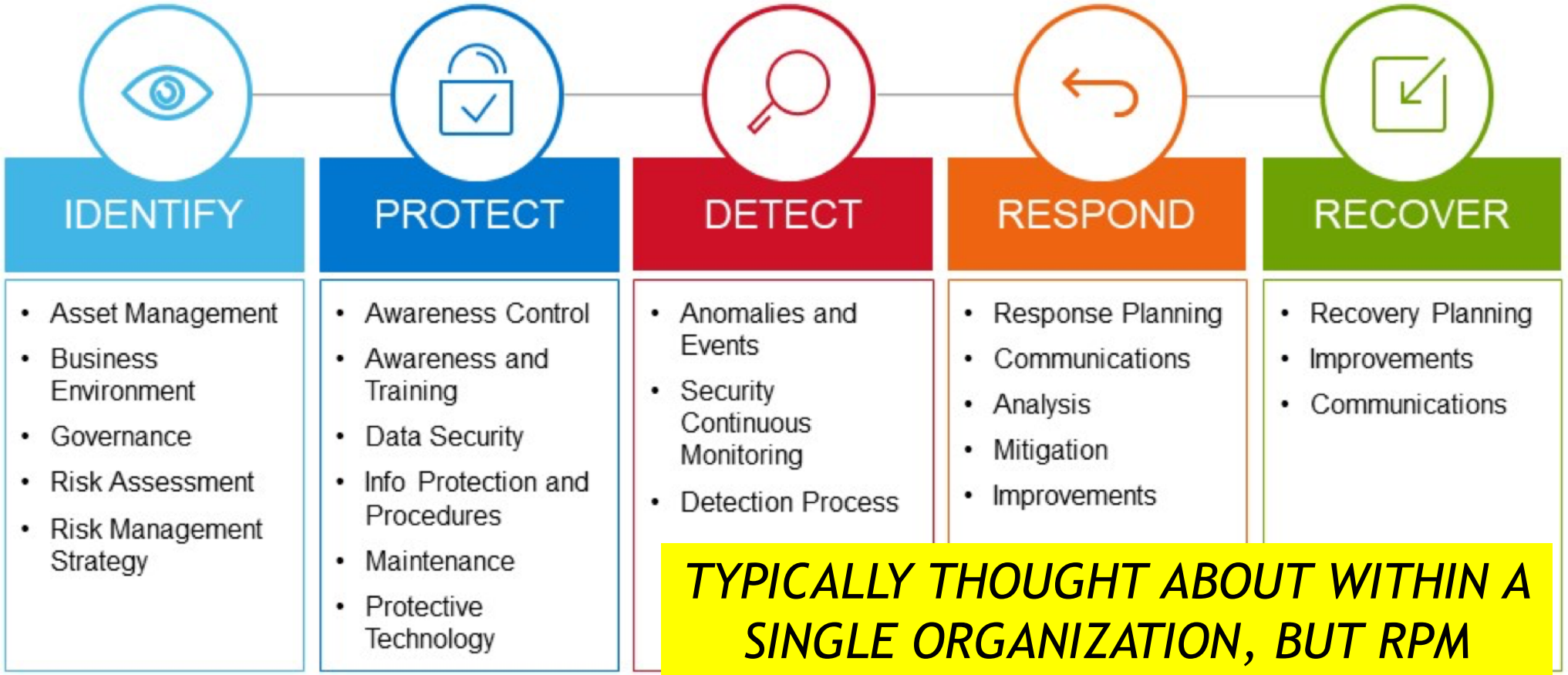


https://www.nist.gov/news-events/news/2019/06/connecting-iot-device-check-out-new-nist-report-cybersecurity-advice

Risk Assessment

1. Characterize the System
2. Identify Vulnerabilities
3. Identify Threat Sources and Events
4. Determine Likelihood of Occurrence (Exploit)
5. Determine Magnitude of Impact
6. Calculate Risk (Likelihood x Impact = Risk)
7. Analyze Controls
8. Consider Residual Risks

NIST Cybersecurity Framework Overview



TYPICALLY THOUGHT ABOUT WITHIN A SINGLE ORGANIZATION, BUT RPM REQUIRES THINKING ABOUT A SYSTEM OF SYSTEMS

https://www.nist.gov/cyberframework

PLATFORM PROVIDER

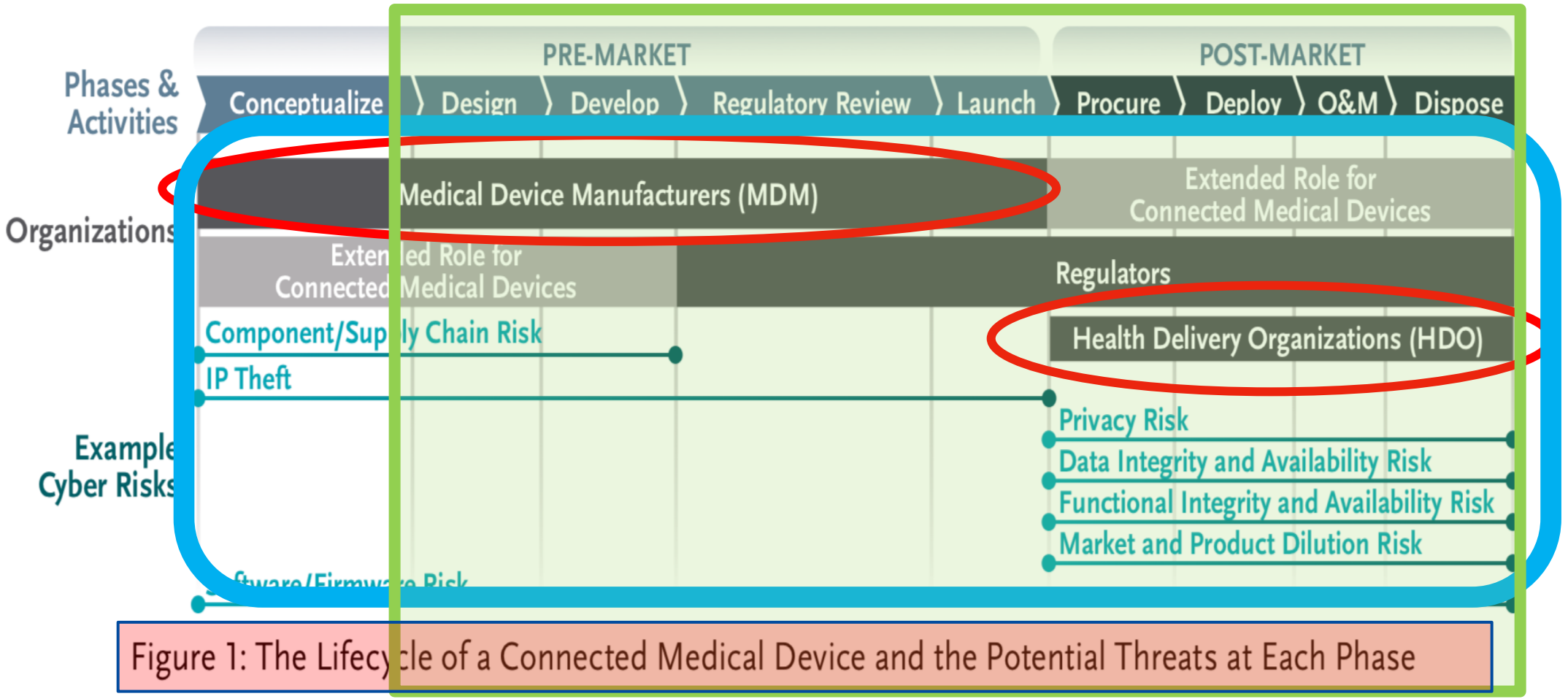


Figure 1: The Lifecycle of a Connected Medical Device and the Potential Threats at Each Phase

Securing Connected Medical Devices FINAL 10.28.19.pdf
https://www.ehidc.org/sites/default/files/resources/files/Securing%20Connected%20Medical%20Devices%20FINAL%2010.28.19.pdf

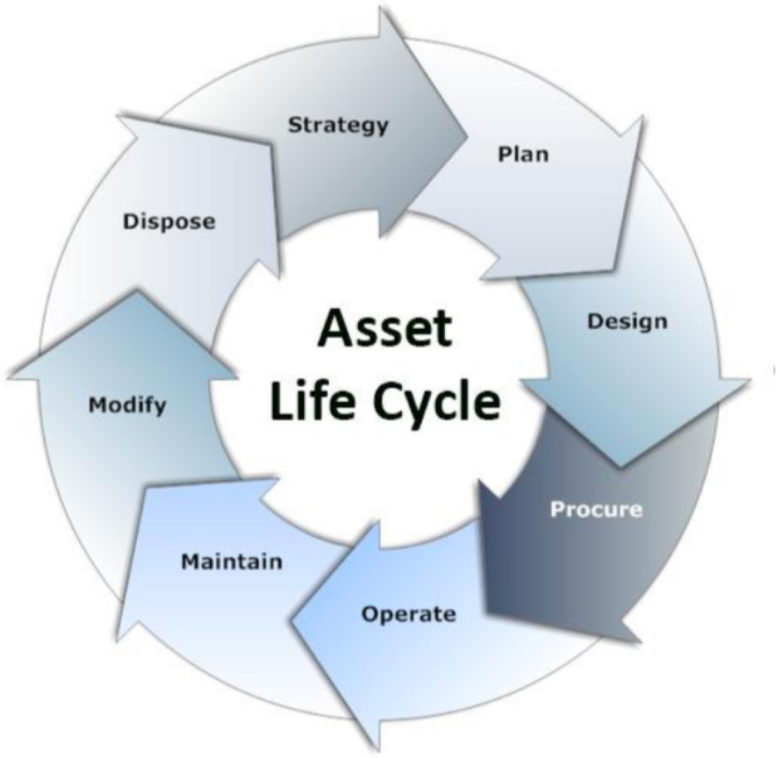
eHealth Initiative and Foundation

Best Practices

Vendor Security Assessment

1. what data is transmitted?
2. what data is stored?
3. what data is processed?
4. how do devices connect to the vendor?
5. how does the vendor connect to your organization?
6. network diagram
7. flow diagram
8. storage diagram
9. what cybersecurity and privacy policies and procedures are in place?
10. what logging and monitoring are in place?
11. what sort of vulnerability management program exists?
12. what is the program to keep software updated and patched?
13. is there an intrusion detection system?
14. is there file integrity monitoring?
15. is there an incident response plan?
16. what industry cybersecurity standards are followed?
17. what independent cybersecurity review has been done?
18. is there a security awareness program?
19. is there an annual cybersecurity risk assessment?
20. are annual penetration tests conducted?
21. how does the vendor assess the security of its partners and suppliers?

Life Cycle View

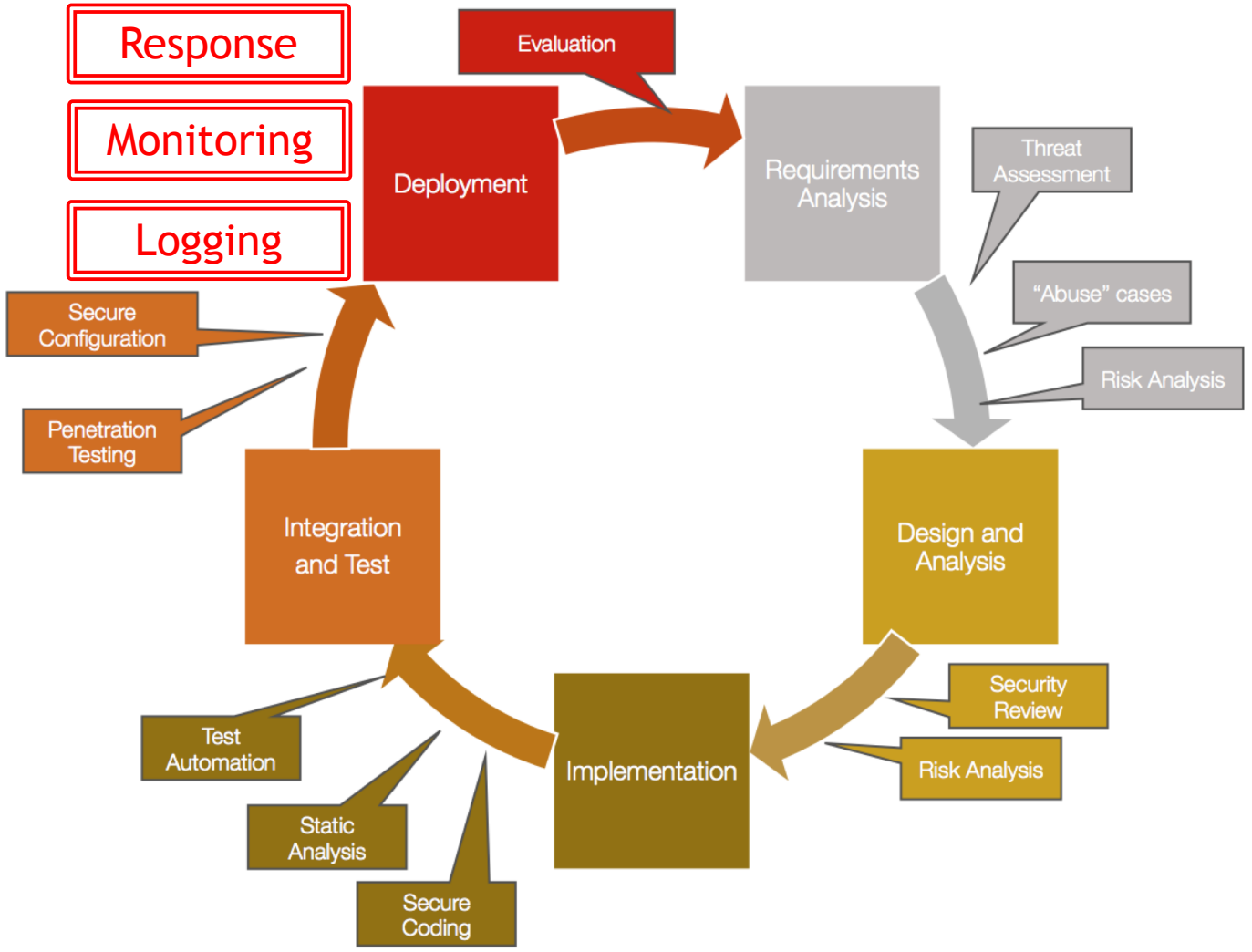


- Design
- Build
- Deploy
- Operate
- Maintain
- Decommission

Designing Security In…

Updating

Patching



https://blogs.grammatech.com/designing-security-into-medical-device-software

Design

- Require authentication
- No default usernames or passwords
- Only connect when needed
- Encrypt transmissions
- If possible, avoid storing confidential information
  - If storage is necessary, encrypt
- Enable logging, monitoring, updating, and patching
- Plan for secure decommissioning

Build

- Supply chain security, including Bill of Materials/ SBOM
- Secure conditions for injecting encryption keys
- Tamper resistance

Deploy

- Secure delivery
- Change userids and passwords during setup
- Provide technical support for unsophisticated end users

Operate

- Logging
- Monitor for aberrant communications (interruptions or unauthorized)

Maintain

- Install updates as needed (securely)
- Install patches as needed (securely)

Test

- Test for calibration, connection, and integrity
- Periodic third-party evaluation of security and reliability
  - Vulnerability scans
  - Penetration tests

Intrusion Detection/Incident Response

- How will you detect attacks and compromises?
- What is your plan to respond?
- Roles and responsibilities?
  - HDO – Platform - Home health service - Manufacturer
- How will you train?
- How will you test?
  - Table top exercises
  - Full-scale exercises

Decommission

- Delete Personal Health Information (PHI) and Personally Identifiable Information (PII)
- Delete authentication and authorization codes

Wrapping Up & Getting Ready for Q & A

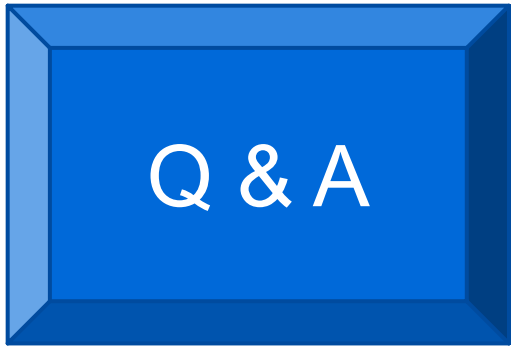
This Presentation

- Introductions & Context
- How RPM Works
- System of Systems / Teamwork
- Vulnerabilities, Threats, and Attacks
- Risk Assessment
- Best Practices
- References

42TEK, Inc.

To request information or to collaborate, use Contact Form at www.42tek.com

Program management & product development for data security, healthcare systems, critical infrastructure, and electronic payments.



David Snyder, MBA, PE, CISSP, CSM

www.42tek.com david@42tek.com

References

- Securing Telehealth Remote Patient Monitoring Ecosystem, NIST NCCoE, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf
- NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, NIST, https://doi.org/10.6028/NIST.IR.8228
- Telemedicine Toolkit, AHIMA, https://healthsectorcouncil.org/wp-content/uploads/2018/08/AHIMA-Telemedicine-Toolkit.pdf
- Validating the Integrity of Servers and Client Devices, NIST NCCoE, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/tpm-sca-draft-project-description.pdf
- Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices, FDA, https://www.fda.gov/media/95636/download

- Health Care Industry Cybersecurity Task Force June 2017 Report on Improving Cybersecurity in the Health Care Industry https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf
- Healthcare and Public Health Sector Coordinating Council, Medical Device and Health IT Joint Security Plan, January 2019 https://healthsectorcouncil.org/the-joint-security-plan/
- The FDA's Role in Medical Device Cybersecurity, *Dispelling Myths and Understanding Facts* *https://www.fda.gov/media/103696/download*
- MITRE, Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

- “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0
- “Postmarket Management of Cybersecurity in Medical Devices” https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
- “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices” (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/u cm089543.htm)

- “Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software” (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/u cm077812.htm)
- Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication (2013) http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm?source=govdelivery
- Cybersecurity for Networked Medical Devices is a Shared Responsibility: FDA Safety Reminder (updated Oct. 2014) http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm

- Medical Device Software Patching, IHE PCD in Cooperation with MDISS (Oct. 2015),http://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Patching_Rev1.1_2015-10-14.pdf
- Medical Equipment Management, Medical Device Cyber Security Best Practice Guide, IHE PCD (Oct. 2015), http://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf
- Medical Equipment Management, Cyber Security, IHE PCD (May 2011), http://ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05- 27.pdf
- Building Code for Medical Device Software Security, IEEE Computer Society, May 2015, http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf

- Medical Device Isolation Architecture Guide, V2.0, US Department of Veterans Affairs (Aug. 2009), http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf
- VA Enterprise Design Patterns Privacy and Security - Medical Device Security, Jan 2017 https://www.oit.va.gov/library/programs/ts/edp/privacy/MedicalDeviceSecurity_V1.pdf
- “Medical Devices Security Technical Implementation Guide, V1, R1” Defense Information Systems Agency (DISA), July 2010, http://iase.disa.mil/stigs/Documents/unclassified_medical_device_stig_27July2010_v1r1FINAL.pdf
- Medical Devices Security Technical Implementation Guide, V1 R1, Defense Information Systems Agency (DISA) (July 2010), http://iase.disa.mil/stigs/Documents/unclassified_medical_device_stig_27July2010_v1r1FINAL.pdf

- Manufacturer Disclosure Statement for Medical Device Security, NEMA (Oct. 2019); https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
- ANSI UL 2900-2-1 First Edition 2017 Standard For Safety, Software Cybersecurity For Network-Connectable Products, Part 2-1: Particular Requirements For Network Connectable Components Of Healthcare And Wellness Systems https://standardscatalog.ul.com/standards/en/standard_2900-2-1_1
- ANSI UL 2900-1 First Edition 2017 Standard For Safety, Standard For Software Cybersecurity Network-Connectable Products, Part 1: General Requirements https://standardscatalog.ul.com/standards/en/standard_2900-1_1
- Patching Off-the-Shelf Software Used in Medical Information Systems, NEMA/COCIR/JIRA Security and Privacy Committee, Oct. 2004, http://www.medicalimaging.org/wp-content/uploads/2011/02/Patching_OffTheShelfSoftware_Used_in_MedIS_October_2004.pdf
- Office of Inspector General: FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices: https://oig.hhs.gov/oei/reports/oei-09-16-00220.pdf

- I Am The Calvary “Hippocratic Oath for Connected Medical Devices” https://www.iamthecavalry.org/domains/medical/oath/
- MedCrypt: What Medical Device Vendors can learn from past Cybersecurity Vulnerability Disclosures https://www.medcrypt.co/medcrypt-vulnerability-analysis-whitepaper-1.pdf
- Medcrypt: A Medical Device Cybersecurity Toolbox https://www.medcrypt.com/whitepapers.html
- Medcrypt: A Tool in Medical Device Cybersecurity https://www.medcrypt.com/whitepapers.html
- Medcrypt: Impact of Monitoring on Medical Device Vulnerabilities https://www.medcrypt.com/whitepapers.html

- “Anatomy of an Attack – Medical Device Hijack (MEDJACK)”, TrapX, 2015 https://trapx.com/trapx-labs-report-anatomy-of-attack-medical-device-hijack-medjack/
- “MEDJACK 2: Old malware used in new medical device hijacking attacks to breach hospitals”; Network World; Jun 27, 2016; http://www.networkworld.com/article/3088697/security/medjack-2-old-malware-used-in-new- medical-device-hijacking-attacks-to-breach-hospitals.html
- “Securing Hospitals – A Research Study and Blueprint”, Independent Security Evaluators (ISE), Feb. 2016, https://www.securityevaluators.com/hospitalhack/
- ISO 13485, *Medical devices – Quality management systems – Requirements for regulatory purposes* *https://www.iso.org/iso-13485-medical-devices.html*

- OWASP Secure Medical Device Deployment Standard, Version 1.0 9/12/17 https://www.owasp.org/images/7/73/MedicalDevicePurchasing.pdf
- OWASP OWASP Secure Medical Device Deployment Standard: Purchasing Assessment Criteria Version 1.0 9/12/17 https://www.owasp.org/images/7/73/MedicalDevicePurchasing.pdf
- AAMI TIR57: Principles for medical device security—Risk management https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729&gclid=EAIaIQobChMIz7-J7cKX5AIVhobACh30Bw-_EAAYASAAEgIwPPD_BwE
- AAMI Medical Device Cybersecurity: A Guide for HTM Professionals https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=6489

- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST SPECIAL PUBLICATION 1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf
- MAUDE - Manufacturer and User Facility Device Experience https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM
- FDA: Recognized Consensus Standards https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm [search terms: risk; device; cybersecurity]

- Selection of Cybersecurity-Related Standards in Development for Medical Devices https://www.fda.gov/media/123070/download
  - **ISO/IEC 81001-1 Health software and health IT systems safety, effectiveness, and security – Part 1: Foundational principles, concepts and terms**
  - **IEC 80001-5-1 Safety, effectiveness, and security in the implementation and use of connected medical devices or connected health software – Part 5: Security – Part 5-1: Activities in the product lifecycle**
  - **IEC 60601-4-5 Guidance and interpretation – Safety related technical security specifications for medical devices**
  - **IEC 62304 Medical device software – Software life cycle processes**
  - **AAMI TIR97/Ed. 1, Principles for medical device security – Post-market security management for device manufacturers**
  - **AAMI SW96/Ed. 1, Medical Devices – Application of security risk management to medical devices**