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
HOW I GOT HERE

RESPIRATORY THERAPY

ENVIRONMENTAL INVESTIGATIONS
FIELD & LAB DATA

CREDIT CARD SYSTEMS
Remote Patient Monitoring was imagined long ago...
Arno Krugel, The doctor of the future, Stuttgart 1924
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
RISE IN VIDEO HOUSE CALLS TO AVOID HOSPITAL VISITS
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

HEART DISEASE
CANCER
CHRONIC LUNG DISEASE
STROKE
ALZHEIMER’S DISEASE
DIABETES
CHRONIC KIDNEY DISEASE
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.

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)
  

- Additional information at
  
State Medicaid & CHIP Telehealth Toolkit
Policy Considerations for States Expanding Use of Telehealth
COVID-19 Version

CARES Act Expands Medicare Telehealth Coverage for Medicare and the VA

The Coronavirus relief bill passed by Congress and signed by President Trump last week expands Medicare coverage for telehealth, allowing FQHCs and RHCs to qualify for coverage and boosts funding for broadband services.

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

CPAP machines may also be among the high numbers.
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 RPM model

Figure 3-1: High-Level Architecture
Alternate Model

- BLUETOOTH
- USB
- ETHERNET
- SERIAL
- CELLULAR

HUB

CELLULAR CARRIER

CLOUD SERVICE

Or land line
<table>
<thead>
<tr>
<th>Connectivity Option</th>
<th>Hardware</th>
<th>Home Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>LATITUDE Ethernet Adapter or Wireless Internet Adapter</td>
<td>Requires access to high speed Internet modem/router</td>
</tr>
<tr>
<td>Cellular</td>
<td>LATITUDE Cellular Adapter</td>
<td>Service provided by AT&amp;T and T-Mobile</td>
</tr>
<tr>
<td>Landline</td>
<td>Included with the LATITUDE Communicator</td>
<td>Compatible with most analog and digital phone services</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Differences</th>
<th>Hospital</th>
<th>Remote Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Often capital equipment</td>
<td>Expense item</td>
</tr>
<tr>
<td></td>
<td>Long useful life</td>
<td>May not have long life</td>
</tr>
<tr>
<td></td>
<td>On-site IT &amp; clinical engineers</td>
<td>No on-site support</td>
</tr>
<tr>
<td></td>
<td>Logging &amp; monitoring</td>
<td>Logging/monitoring less likely</td>
</tr>
<tr>
<td></td>
<td>Network segmentation possible</td>
<td>Typically cloud platform</td>
</tr>
<tr>
<td></td>
<td>Many people around</td>
<td>Few people around</td>
</tr>
</tbody>
</table>

© 42TEK, Inc.
“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.

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

COLLECTED

TRANSMITTED

STORED & PROCESSED

COLLECTED

TRANSMITTED

STORED & PROCESSED

Or land line

© 42TEK, Inc.
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

© 42TEK, Inc.
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
- Healthcare Delivery Organization IT staff
- Healthcare Delivery Organization clinical engineers
- Clinical staff
- Food & Drug Administration
- Federal Communications Commission
- Standards organizations
“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.”

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 an entry point for gaining entry to hospital network
Cybersecurity is Not Just About Attacks

It’s also about compatibility and interoperability

COVIDSafe may interfere with diabetes-monitoring apps

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.

- **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.
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.
The databases storing RPM data

Mistakes by people

- Device
- Home Network/Smartphone
- Carrier/ISP
- Cloud Platform
- Healthcare Delivery Organization
- Home Health Provider
- Supply Chain
- Manufacturer
- Distributor

© 42TEK, Inc.
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.”

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?

- BLUETOOTH
- USB
- ETHERNET
- SERIAL
- CELLULAR

Or land line
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
What capabilities do IoT devices have?

What are their cybersecurity and privacy risks?

What challenges are there for mitigating these risks?

How might an organization address these challenges?

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
TYPICALLY THOUGHT ABOUT WITHIN A SINGLE ORGANIZATION, BUT RPM REQUIRES THINKING ABOUT A SYSTEM OF SYSTEMS
Figure 1: The Lifecycle of a Connected Medical Device and the Potential Threats at Each Phase
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
- Response
- Monitoring
- Logging
- Secure Configuration
- Penetration Testing
- Integration and Test
- Test Automation
- Static Analysis
- Secure Coding
- Deployment
- Evaluation
- Requirements Analysis
- Threat Assessment
- "Abuse" cases
- Risk Analysis
- Design and Analysis
- Security Review
- Risk Analysis

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 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

- NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, NIST, [https://doi.org/10.6028/NIST.IR.8228](https://doi.org/10.6028/NIST.IR.8228)


- **Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices**, FDA, [https://www.fda.gov/media/95636/download](https://www.fda.gov/media/95636/download)
- Health Care Industry Cybersecurity Task Force June 2017 Report on Improving Cybersecurity in the Health Care Industry
- 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


“Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices” ([http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm))
“Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”
(http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.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


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

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

“MEDJACK 2: Old malware used in new medical device hijacking attacks to breach hospitals”; Network World; Jun 27, 2016;


- OWASP Secure Medical Device Deployment Standard, Version 1.0 9/12/17
  [https://www.owasp.org/images/7/73/MedicalDevicePurchasing.pdf](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](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-J7cKX5AIVhobACCh30Bw-_EAAYASAAEglwPPD_BwE](https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729&gclid=EAIaIQobChMIz7-J7cKX5AIVhobACCh30Bw-_EAAYASAAEglwPPD_BwE)

- AAMI Medical Device Cybersecurity: A Guide for HTM Professionals
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology

- NIST SPECIAL PUBLICATION 1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

- MAUDE - Manufacturer and User Facility Device Experience

- 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