HIMSS Cybersecurity Community Sponsor

Future Evolution of the Hospital Command Center

Mitchell Parker, IU Health

Indiana University Health

Introduction

- As we continue to deal with the changes from COVID-19, one stands out the most
- Hospitals and health systems have now embraced telemedicine and remote monitoring
- A year ago, this would have been thought unthinkable. Now, this is something that we manage as part of business

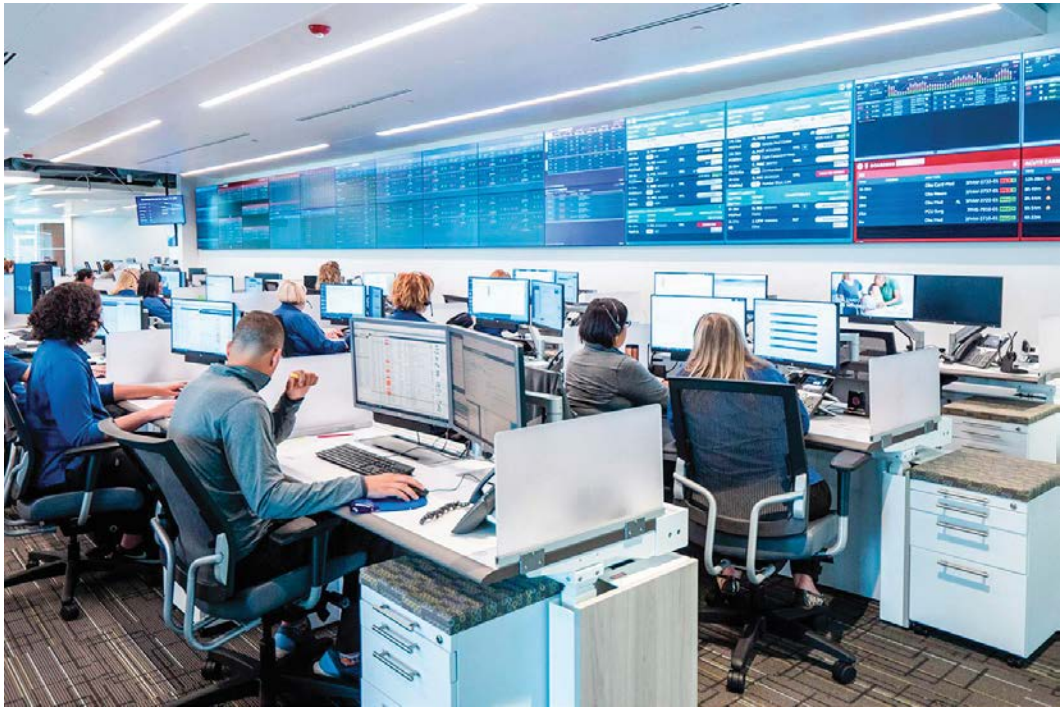
Why are we here?

- This presentation will cover the concepts of how a Hospital Command Center can integrate IoMT security into their processes.
- It will cover how latency in existing “smart cities” implementations and protocols, often touted as the archetype to build from:
  - Do not meet the needs of hospitals
  - And how newer wireless technologies combined with secure Application Programming Interfaces can
- We will build from the ground up for devices and show what needs to happen to be effective in implementing this
- First, we’ll start with some basics…

What is a command center?

- According to Mandy Roth - https://www.healthleadersmedia.com/innovation/move-over-star-wars-hospital-command-centers-take-spotlight
- A Command Center is a centralized location that manages the complex operations of a healthcare organization via cooperation and collaboration
- First accomplished by Johns Hopkins in 2016 and improved on by many
- They use real-time information about incoming patients, ED and OR capacity, bed availability, and discharges
- They use advanced analytics and intelligent systems to help perform analysis on the numerous data points
- Tampa General Hospital uses these to increase care coordination, patient safety and quality, and to improve efficiency

Example Hospital Command Center



What are ”Smart Cities”

- According to the paper Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation:
  - It focuses on the latest advancements in mobile and pervasive computing, wireless networks, middleware and agent technologies as they become embedded into the physical spaces of cities.
  - Used to mobilize cities and urban environments for change and innovation

What are their limitations when applied to healthcare?

- According to the paper Internet of Things for Smart Cities, by Zanella, Bui, Castellani, Vangelista, and Zorzi:
  - Low traffic rate (packets per minute)
  - High tolerable delay for smart devices (minutes)
  - Feasibility dependent upon infrastructure
  - Transmission security not even considered
  - Low complexity of services
- Healthcare requires high traffic rate and low latency (seconds at most)
- HIPAA requires the use of transmission security with PHI
  - Else you have transmissions intercepted like pagers

What are our challenges?

- Minimize the use of scarce resources, esp. PPE
- Adapt to the rapid adoption of telemedicine and remote services
- Effectively monitor these services to deliver superior quality
- Deliver a superior quality service and better experience
- Secure data provenance from device to Electronic Health Records
- Ensure that we address technology issues before they become something much worse

What do we have to do?

- Take a job that has normally been the provenance of skilled practitioners and move it out of the four walls of the facility into the community
- Do so with introducing as little risk as possible
- Preserve scarce resources for the most critical needs
- Give you a playbook you can use to build your own or integrate into your command center

What does this take?

- Understanding what devices we have in our inventory and their capabilities
- Ensure they are properly placed and have good connectivity
  - Utilize new technologies to monitor them
- Monitor the devices monitoring our patients to ensure proper operation
  - Verify and validate data coming from the devices
- Develop plans to address when undesired outcomes happen
- Develop plans to accommodate patients when either connectivity or the devices fail

Won't 5G fix it?

- 5G is just a transport medium
- It addresses latency from the phone to the Internet
- It is dependent upon the Internet and phone systems
  - If there's a bad Internet connection to you this doesn't solve for that
- While it is designed to have better security, higher speeds, and lower latency, it doesn't provide significant benefits for monitoring or command centers
  - Which a 4G/LTE connection can still do very well
- When network slicing becomes more popular with 5G we will see major security improvements for device connectivity

Won't 5G fix it?

- However, since 5G devices still have to send data to services using APIs or standard TCP/IP connections, the risk there is not migitated
- We need to be even more vigilant than before regarding API and TCP/IP endpoints as there is still a major security risk
  - 5G does not make you instantly more secure
- Be wary of anyone claiming that 5G will make for a better command center
- It does well for transporting data, however, it's not a cure-all for inattention to operational management

Won't AI fix it?

- No
- AI, machine learning, intelligent systems, and advanced analytics are excellent for spotting patterns and inferring conditions when humans cannot
- While these technologies are an important component, they need to be backed by playbooks and processes
- We need to check for false positives and false negatives
- AI can't yet follow through and actually implement the work
  - Will that practically happen in our lifetimes? Maybe

What will fix it?

- A command center is designed to help people make more informed decisions to guide the actions of others for better and more beneficial outcomes
- It is designed to foster and facilitate cooperation and collaboration by having groups of people work together in an interactive environment using data and analytics to solve problems
- Data is the key to success
- Including security helps us address issues caused by an overly complex technical environment by providing an environment to address these issues at their root

What are we going to cover?

- We're going to discuss the thought processes that need to be considered to integrate processes into a command center
- The goal of what we're doing is to get you to consider multiple categories so that you can make more thoughtful and informed decisions on how to manage your command center processes
  - And increase your probability of success

What do we need to know about each IoT device?

- Normal State
- Exceptions
- Security Exceptions for the device and connecting/routing equipment
- What to do when exceptions occur
  - Internet
  - Phone System
  - Device
  - Security
- Who to send out when they occur?

What do we need to know about each IoT device?

- Alternative Mode Operations until we can get them back up
  - Including and especially device security
  - What happens if there's a patient that needs 24/7 monitoring?
    - We may need to bring them in
  - What happens when there's an outage with a major internet or cellular provider?
- How do we handle updates and patches?

What are our concerns?

- People will put in a Command Center that looks good and doesn't serve the need of better outcomes for patients
- COVID has demonstrated the need to remotely protect patients and protect scarce resources
- We need to monitor better to be able to live up to this
- We must have action plans for when automated monitoring fails and a patient is at risk
- We have to develop and execute operational plans on each device we monitor in a command center, like a security playbook for a detected threat

Answering simple questions

- We listened in our 4th grade classes
- A major part of security success is rooted in answering simple questions about complex problems
- We broke this down to the Who, What, When, Where, Why, and How
- The end goal is to get you to answer simple questions about device monitoring as part of a Hospital Command Center
- Use these simple questions to build use cases for your team
- We will give the example of a CPAP machine at the end to work through the problem as an example

Who

- Who is this device monitoring?
  - What characteristics does the typical subject using this device have?
- Who responds in the case of an adverse event?
  - How long do they have to respond to these event types?
    - Connectivity Interruptions
    - Device Security Issues
    - Device Breakage
    - Abnormal Events
    - Other events

Who

- Who do we partner with to address concerns?
  - Patient Transport
  - Overflow facilities for monitoring
  - Device Repair
  - Information Security Team
  - Escalation for medical issues

What

- What conditions is this device monitoring for?
- What do we need to monitor?
  - Event data
  - Event conditions
  - Device connectivity
  - Normal Events
  - Abnormal Events

What

- What do we do when an abnormal event happens?
  - What to do when exceptions occur
    - Internet
    - Security
    - Phone System
    - Device
- What does an abnormal event mean?
- Who to contact or send out when they occur based on the event?

What

- What Alternative Mode Operations do we use until we can get them back up?
  - Including and especially device security
  - What happens if there's a patient that needs 24/7 monitoring?
    - We may need to bring them someplace that can monitor them
  - What happens when there's an outage with a major internet or cellular provider?

When

- When/how often do we poll or monitor them?

Where

- Where are they located?
- Where are the resources that can help us located?
- Where are the security protections located?
  - On the device itself
  - On a device functioning as a router for transmissions
  - In transport
  - At the receiving end

Why?

- Why are we monitoring them?
- Why did we make the decision to remotely monitor them?
- Why did we think they would be good candidates to be monitored in a command center?

How

- How much bandwidth do they take?
- How much latency is tolerable?
- How do we assure integrity and security of the data?
- How do we authenticate and verify users?
- How do we handle updates and patches?
- How do we demonstrate success?
- How do we alert subjects to issues?
  - What instructions do we give?

How

- How do we demonstrate success in dealing with adverse conditions?
  - Utilize Failure Mode and Effects Analysis to map out where the failures can occur
  - Develop countermeasures to address them

CPAP Use Case Questions

- Who is this device monitoring?
  - Patients with difficulty breathing when they are sleeping
  - These are people who often have sleep apnea or other complicating factors
- Who responds in the case of an adverse event?
  - If this is an abnormal event where someone can't breathe and the device sends an alarm, you need to send over medical assistance
  - If this involves lack of connectivity, you need to make sure they have a way of recording compliance
  - If the patient figures out how to unlock the device, you need to put that at the right approved setting

CPAP Use Case Questions

- If the device breaks, you need to send out a tech to replace the device and configure the settings correctly
- If an event that does not match the above happens, you need to send out a tech to examine the device and potentially replace it

CPAP Use Case Questions

- Who do we partner with to address concerns?
  - Do we partner with a Durable Medical Equipment manufacturer to service these devices or do we do this ourselves?
  - Do we have staff able to monitor for compliance?
  - Who do we call if patients have medical issues based on their location?

CPAP Use Case Questions

- What conditions is this device monitoring for?
  - This monitors for sleep apnea or other breathing conditions requiring constant airflow
- What do we need to monitor?
  - Device Serial Number and Settings
  - Condition
  - Start Date
  - How long therapy lasted
  - Abnormal alarm conditions
  - Network connectivity for cell-enabled models
  - SD card status

CPAP Use Case Questions

- What does an abnormal event mean?
  - The device is not capable of delivering air
  - The device sends out an alert that it is not able to deliver air
  - The device detects that the patient is having an adverse condition
  - The device sends out an alert that its security has been compromised
  - The device sends out an alert that someone has logged in and changed settings

CPAP Use Case Questions

- What do we do when an abnormal event happens?
  - If it is life-threatening, get medical assistance over to their house
  - If it isn't, schedule an appointment with the DME provider to look at the machine
- If there's an Internet/network connectivity exception, make sure there's an SD card in the machine capable of storing session data
- If there's a security exception, send to the Information Security team for triage and schedule an appointment for DME replacement and device forensics
- If there's a device issue, send out someone from DME replacement

CPAP Use Case Questions

- What Alternative Mode Operations do we use until we can get them back up?
  - Have them do something different
  - If it's determined to require additional services, have a plan to get them to that place
- When/how often do we poll or monitor them?
  - Beginning, after, and during the session if the machine supports it

CPAP Use Case Questions

- Where are they located?
  - Do we have their current home address?
- Where are the resources that can help us located?
  - Do we have local EMS, the nearest repair tech, and support reps in the system?
- Where are the security protections located?
  - Do we have protection on the device and its wireless interfaces?
  - Does it use TLS to encrypt data in transit?
  - Do we have it at the receiving end of the APIs?

CPAP Use Case Questions Here

- Why are we monitoring them?
  - Because it helps them improve their condition
- Why did we make the decision to remotely monitor them?
  - To provide a higher quality of life and keep them in a familiar environment
- Why did we think they would be good candidates to be monitored in a command center?
  - So we can monitor many at the same time and be able to more efficiently handle adverse conditions through collaboration and communication
  - Including IoT Security issues

CPAP Use Case Questions

- How much bandwidth do they take?
  - 2Kb total per session, plus 5k for checksums
- How much latency is tolerable?
  - 1-2 s
- How do we assure integrity and security of the data?
  - TLS encryption of data
- How do we authenticate and verify users?
  - Through Device ID assigned to use in the health record

CPAP Use Case Questions

- How do we handle updates and patches?
  - The Service Tech uploads them via SD card
- How do we demonstrate success?
  - Improved compliance rates
  - Improved response time to critical issues
- How do we alert subjects to issues?
  - Phone calls, messages, alerts to them or alternate contacts
  - What instructions do we give?
    - Depends on the situation and advice of staff

What are the expected outcomes?

- A command center that integrates security as part of the process
- One that truly extends services
- A higher quality of service
- More forethought to how to integrate other than statues and blinking lights like everyone else has

Thank you!

- Questions at the end