The Internet of (Health) Things:

*Incorporating IoT Devices into Provider Networks*

*July 10, 2018*
June 2017 – HHS Report on Improving Cybersecurity

"[F]or the health care industry cybersecurity issues are, at their heart, patient safety issues .... health care cybersecurity is a key public health concern ...."

The issue: (1) deep digital connectivity necessary for patient care; but (2) non-secure connections can "betray patient safety."

The problem: "Healthcare cybersecurity is in critical condition."
- "Severe" lack of security talent
- Legacy equipment
- Premature or over-connectivity (driven by meaningful use requirements)
- Epidemic of known vulnerabilities
- Vulnerabilities impacting patient care
June 2017 – HHS *Report on Improving Cybersecurity*

"[F]or the health care industry cybersecurity issues are, at their heart, patient safety issues .... health care cybersecurity is a key public health concern ...."

The **ecosystem:**

- Unique culture
- Digital transformation
- Regulatory environment
- Varying organizational size, resources
- Risks in addition to patient care
- Disclosing vulnerabilities is complex
June 2017 – HHS Report on Improving Cybersecurity

"[F]or the health care industry cybersecurity issues are, at their heart, patient safety issues .... health care cybersecurity is a key public health concern ...."

The solution (?): Six "imperatives"

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks and exposure.
6. Improve information sharing of industry threats, weaknesses, and mitigations.
2018 HIMSS Cybersecurity Survey

• Most HCOs (76%) had a “significant” security incident in the past 12 months

• We’re moving in the right direction ...

• ... but there’s room to improve
2018 HIMSS Cybersecurity Survey

- Security incidents
- Progress
- Vulnerabilities
IoHT: What is it?

"[T]he integration of the physical and digital worlds through objects with network connectivity in the healthcare industry."

What can it do?

- Increase access to healthcare
- Improve patient outcomes
- Engage providers
- Reduce healthcare costs
- Enhance consumer experience
- Heighten operational efficiency

Hospitals use it for ....

- Remote patient monitoring
- Wellness and prevention
- Operations

*Accenture LLP
Getting Started: Develop a Risk Management Policy

- Balance safety, efficacy, cybersecurity with provider’s mission
- Establish risk acceptability criteria for safety, efficacy, cybersecurity
- Describes processes for medical IT networks
  - Event management
  - Change management
  - Configuration management
  - Monitoring
Getting Started: Medical IT System RM Files

Documents:

• Manufacturer-supplied materials
• Asset information
• Configuration management information
• Responsibility agreements with all relevant stakeholders

Trace each identified system vulnerability to:

• Risk analysis
• Risk management plan
• Implementation/verification of control measures
• Residual risk acceptance with appropriate approvals
Getting Started: **Inventory System Assets**

- Medical IT network components and all attached devices
- Operational characteristics of IT infrastructure
- Configuration management information
- Client/server structure
- Healthcare app software
- Data created, maintained, transmitted
- Operating and service history
- Security information (confidentiality, integrity, availability)
- Planned changes, upgrades, enhancements

*Identify and track ....*
Getting Started: Data Mapping

• What devices and networks make up your medical IT system(s)?
• What information do they collect – and why?
• How does the information flow into, through, and out of your organization?
• How do you use the information? Why?
• To whom do you disclose the information? Why?
• Who has access to the information at each stage?

What do you have, where is it stored, how does it move?
Perform a Cybersecurity Risk Analysis

Goal:
An accurate and thorough assessment of potential risks and vulnerabilities that affect data confidentiality, integrity, availability (and resilience).

Method:
• Identify essential device safety and performance levels
• Identify threats and vulnerabilities that impact data confidentiality, integrity, and availability
• Assess likelihood that threat will manifest and exploit vulnerability
• Assess potential impact on confidentiality, integrity, and availability if it does
• Assign risk levels (e.g., high, medium, low)
• Prioritize remediation – focus on essential device safety and performance
Categorize Devices By Risk

- Patient safety impact?
- Process sensitive data?
- Connected to integrated network?
- Likelihood of attack?
- Vendor security SLA?
Common Risk Analysis Pitfalls

- Assuming “IT did it/can do it/will do it”
- Lack of ownership
- Missing RA team members
- Incomplete asset inventory
- Improper asset categorization
- Undervalued assets
- Unidentified vulnerabilities
- Unanticipated threats
- Insufficient likelihood and criticality assessments
- Underappreciated residual risk
- Incomplete or absent documentation
Develop a **Risk Management Plan**

**Goal:**
*Implement security controls sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level.*

**Method:**
- Identify mitigations and compensating controls
  - Do they create new risk?
  - Do they affect device functionality?
- Assess residual risk
- Establish risk acceptance criteria
- Provide end users with relevant information to mitigate risk, make decisions
- Document decisions and rationale
- Present findings and get buy-in
- Regulatory reporting when needed
Buying IoHT Tech: **Smart Contracting**

Goals:
- Identify risk
- Mitigate risk
- Transfer risk

Procurement phases:
- Product evaluation
- Contract negotiation
Buying IoHT Tech: Vetting Vendors

- Framework and standards
- Software/firmware design, development, testing
- Audit controls
- Authorization
- Cybersecurity product upgrades
- Patient data de-identification
- Malware detection/prevention
- Person authentication
- System and application hardening
- Process for vulnerability reporting and remediation
- Health data storage confidentiality
- Transmission confidentiality
Promoting Good Cyber-hygiene

• Your Culture
• Your Network
• Your Processes
• Your Policies
IoHT Cybersecurity: What Can HCOs Do Now?

1. Be flexible and resilient
2. Make cybersecurity part of the framework
3. Identify, educate, and engage leadership
4. Identify and mitigate risks (including residual risk)
5. Develop an investigation and incident response plan (Review, test, evaluate, and modify)
6. Map devices and networks
7. Assign risk categories
8. Consider information-sharing organizations
   - NH-ISAC
   - HPH SCC
   - HITRUST
9. Evaluate vendor contracts
10. Review cybersecurity coverage
QUESTIONS?

Kim Metzger, CIPP/US, CIPM, FIP
Ice Miller LLP
317/236-2296
kimberly.metzger@icemiller.com

Taryn Stone
Ice Miller LLP
317/236-5872
taryn.stone@icemiller.com