Medical Device Cybersecurity for HTM Professionals: An Update on Resources and Practices

Stephen L. Grimes, FACCE FHIMSS FAIMBE
Principal Consultant
Strategic Healthcare Technology Associates, LLC

Axel Wirth, CPHIMS, CISSP, HCISPP
Distinguished Technical Architect
Symantec Healthcare Practice

September 18, 2018 - 12:00 – 1:30 pm

Health Technology ALLIANCE
Advancing the Safety and Security of Devices and Systems

www.HealthTechnologyAlliance.org

Health Technology
ALLIANCE

Advancing the Safety and Security of Devices and Systems

A Collaboration Between

AAMI
Advancing Safety in Healthcare Technology

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

HIMSS®

AAMI
Advancing Safety in Healthcare Technology

Robert D. Jensen

President and CEO

AAMI

http://www.AAMI.org/

Health Technology ALLIANCE

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Arif Subhan, MS, CCE, FACCE

President, ACCE

Chief Biomedical Engineer

VA Greater Los Angeles HCS

https://ACCEnet.org/

Health Technology ALLIANCE

HIMSS

transforming health through information and technology™

Joyce Sensmeier

MS, RN BC, CPHIMS, FHIMSS, FAAN

Vice President, Informatics

Office of the CTIO, HIMSS

www.HIMSS.org

Health Technology ALLIANCE

About the Presenters

Stephen L. Grimes, FACCE, FAIMBE, FHIMSS, is principal consultant in Strategic Healthcare Technology Associates, LLC in Boston, MA. He is a fellow of the American Institute of Medical and Biological Engineering (AIMBE), of the Health Information and Management Systems Society (HIMSS) and the American College of Clinical Engineering (ACCE) where he is also a past president. He has been a prolific writer and speaker on medical device security for nearly 20 years and for over 40 years has served variously as director of clinical engineering at academic medical centers and in management and consulting roles in independent service organizations. He now consults in the areas of HTM strategic and operational issues, technology convergence, security and risk management associated with medical devices and systems, compliance and in quality management.

Health Technology ALLIANCE

About the Presenters

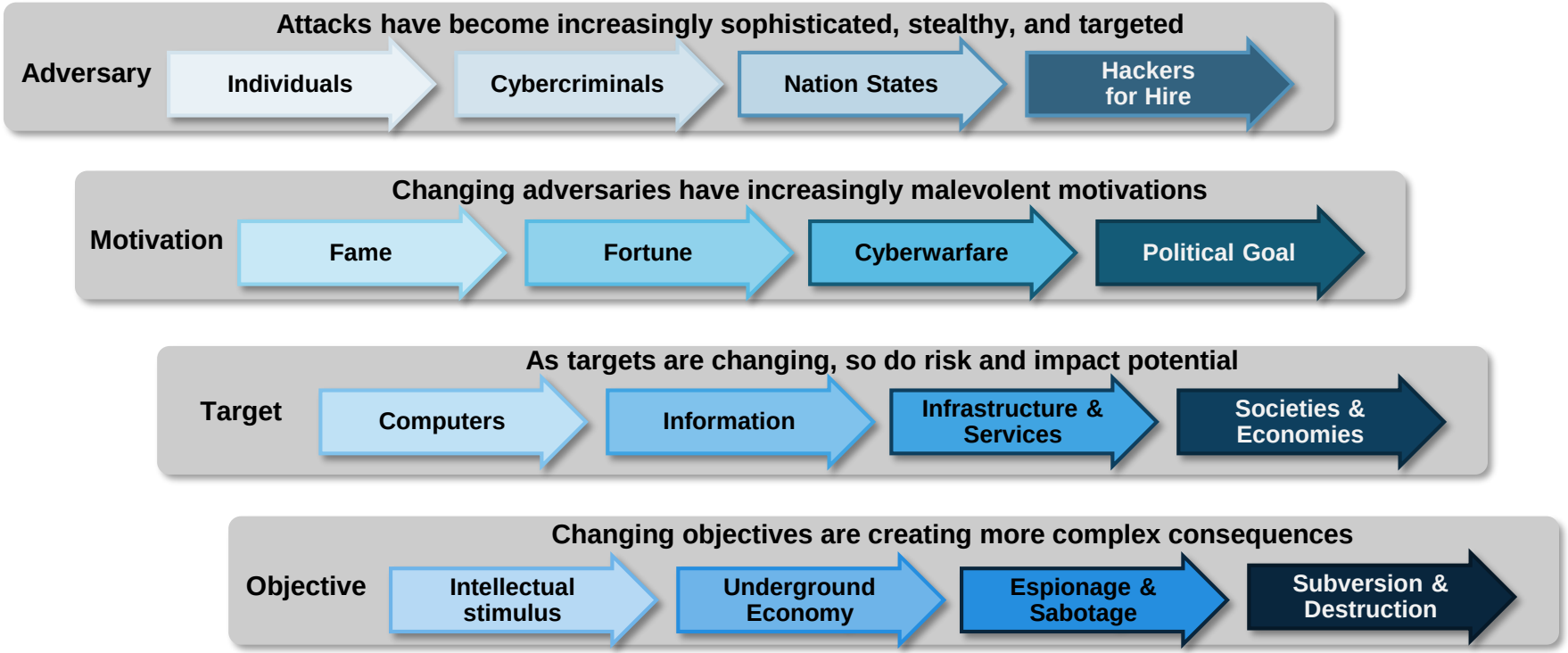
Axel Wirth is a Distinguished Healthcare Architect with Symantec Corporation. He has authored numerous articles, writes an award-winning column for Biomedical Instrumentation & Technology (BI&T), and has frequently presented at ACCE, AAMI, HIMSS, FDA, and NIST webinars and national conferences. He regularly gives lectures to students in graduate clinical engineering programs. Wirth also has been a leader in several national organizations, serving on the AAMI's BI&T editorial board. He is a member of the HIMSS Privacy and Security Committee.

Agenda

- Medical Device Cybersecurity – Why and Why Now?
- Special Issues Affecting Cybersecurity of Medical Devices
- Managing Medical Devices Cybersecurity Risks
- Overview of Resources

Understanding Today's Threats

Changing Adversaries and Objectives



Health Technology ALLIANCE

Symantec 2018 Internet Security Threat Report

The Big Numbers (CY 2017)

Web Threats

More than 1 Billion
Web requests analyzed each day
Up 5% from 2016

1 in 13
Web requests lead to malware
Up 3% from 2016

Email

Percentage Spam Rate

2015	2016	2017
53%	53%	55%

IoT

600%
Increase in Attacks

2016	2017
6K	50K

Vulnerabilities

Overall increase in reported vulnerabilities **13%**

Malware

92%
Increase in new downloader variants

80%
Increase in new malware on Macs

8,500%
Increase in coinminer detections

Ransomware

5.4B
WannaCry attacks blocked

46%
Increase in new ransomware variants

Mobile

Number of new variants

2016	2017
17K	27K

Increase in mobile malware variants **54%**

24,000 Average number of malicious mobile apps blocked each day

29%
Increase in industrial control system (ICS) related vulnerabilities

Cybersecurity Lessons Learned

Cyber incidents can be expensive & cheap doesn't do it

WIRED

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

.....

The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former Homeland Security adviser Tom Bossert, who at the time of the attack was President Trump's most senior cybersecurity-focused official. Bossert and US intelligence agencies also confirmed in February that Russia's military—the prime suspect in any cyberwar attack targeting Ukraine—was responsible for launching the malicious code. (The Russian foreign ministry declined to answer repeated requests for comment.)

To get a sense of the scale of NotPetya's damage, consider the nightmarish but more typical ransomware attack that paralyzed the city government of Atlanta this past March: It cost up to $10 million, a tenth of a percent of NotPetya's price. Even WannaCry, the more notorious worm that spread a month before NotPetya in May 2017, is estimated to have cost between $4 billion and $8 billion. Nothing since has come close. "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says. "That's a degree of recklessness we can't tolerate on the world stage."

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

BBC NEWS

$10 router blamed in Bangladesh bank hack

22 April 2016 | Technology

Better network hardware would have helped police investigate the hack attack, say experts

Hackers managed to steal $80m (£56m) from Bangladesh's central bank because it skimped on network hardware and security software, reports Reuters.

https://www-bbc-com.cdn.ampproject.org/c/s/www.bbc.com/news/amp/technology-36110421

Health Technology ALLIANCE

Medical Devices Under Pressure

Cataclysmic Trends

Public / Health

Changing Care Models
- Reducing cost, increasing efficiency
- Home care, telehealth

Public Awareness:
- Patient are impacted
- Documented care delivery impact
- Headlines & evening news

Regulation & Standards:
- FDA, UL, ISO/IEC, HITECH Act

Ecosystem

Complexity:
- 14 devices/bed; 25%+ networked
- ~12.5M total devices, $110B
- ~8000 manufacturers
- Diversity & dependencies

Longevity:
- 10-20 yr useful life
- Poorly patched, EOL OS's

Security Awareness:
- Designed in a different era
- Traditionally not a decision driver

Significant "Security Debt"
- Change of technology, skills, regulations, process, and culture
- Where do the security $'s come from?

Medical Devices

Adversaries

Changing Threat Landscape:
- Sophisticated, targeted
- Script kiddies to nation states
- Unlimited time and resources

Changing Skills:
- Threshold of doing harm going down
- Underground Economy
- Hackers for Hire

Changing Motivation:
- Destruction and subversion
- Healthcare seen as an easy target

Critical Infrastructure Security:
- DHS, FBI, NIST, HHS

Targeted (malicious) Attacks:
- Patient safety -> national security

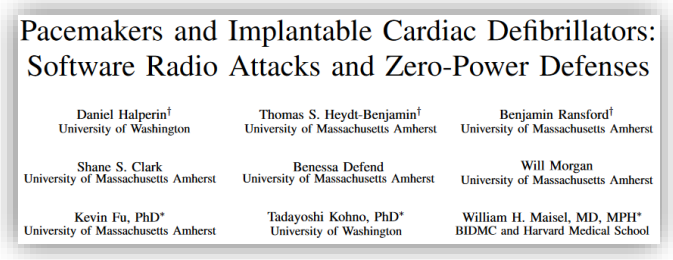
Collateral Damage (nontargeted)
- Common, known vulnerabilities
- Healthcare not unique
- Downtime & care delivery

Risk Awareness

Health Technology ALLIANCE

Medical Device Cybersecurity

Evolution of the topic – More than 10 years in the making



Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin† University of Washington
Thomas S. Heydt-Benjamin† University of Massachusetts Amherst
Benjamin Ransford† University of Massachusetts Amherst
Shane S. Clark University of Massachusetts Amherst
Benessa Defend University of Massachusetts Amherst
Will Morgan University of Massachusetts Amherst
Kevin Fu, PhD* University of Massachusetts Amherst
Tadayoshi Kohno, PhD* University of Washington
William H. Maisel, MD, MPH* BIDMC and Harvard Medical School

Proceedings of the 2008 IEEE Symposium on Security and Privacy

Complexities and dependencies

Early Work (2000 …)

- First reports of network & software induced device malfunction
- AAMI & HIMSS Workshops
- First MDS2 and FDA Guidance on off-the-shelf software

Observation (2008 …)

- Security research: Pacemaker (2008), Insulin Pump (2011)
- Care delivery impact: Med Cabinet (2009), Cathlab (2010)
- More published research; ICS-CERT (multiple warnings, 2013 on)
- FBI Alerts and FDA Warnings on Device Cyber Risks (2015)

Recognition (2012 …)

- IEC 80001 (Risk Management) and MDS^2 (Security Disclosure)
- GAO Report pointing at FDA (2012)
- Industry Initiatives: MDISS, IHE PCD, NIST NCCoE, AAMI
- FDA premarket (2014), postmarket guidance (2016)

Manifestation (2015 …)

- Devices exploited as attack beachhead (TrapX, Protiviti, 2015)
- Providers started device testing; inclusion of security in contracts
- First manufacturers taking the lead (e.g. disclosure policy)
- Vulnerability Sharing (H-ISAC) and Security Certification (UL 2900)

Health Technology ALLIANCE

Medical Device Cybersecurity Ecosystem

Many moving pieces…

Regulatory and Standards Environment (examples)

FDA Pre & Postmarket Guidance
Quality System Regulations / 21 CFR 820
AAMI TIR 57 and TIR 97 (under dev.)

CVSS
H-ISAC (MDSISC)
UL 2900
ICS-CERT

General: CMS/HIPAA, TJC, State Law, etc.
IEC 80001 series
ISO 27799
NIST 1800 series

Manufacturer

- Quality System
- Security Risk Analysis
  - Hazard Analysis (HA)
  - Vulnerability Mgmt. Processes
- Design Security Controls
  - Hardened design
  - HIDS/HIPS
  - Code signing
  - Encryption & Obfuscation
  - Authentication (device, messages)
- Validation and Verification
- Remote access
  - 2FA, VPN, etc.
- Regulatory Filings
  - 510(k), PMA, etc.

Vulnerability Sharing

Threat Intelligence & Security Research

Risk & Incident Sharing

Purchasing Requirements

Security Properties (MDS2, SBoM, HA)

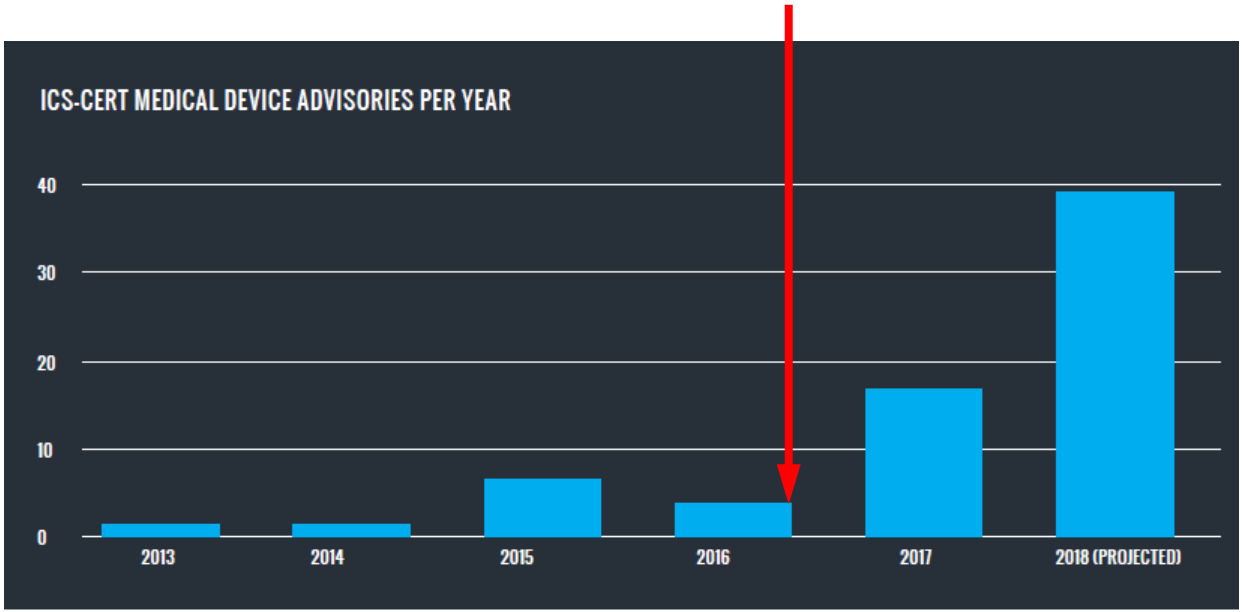
Healthcare Delivery Organization

- Procurement Processes
  - Security requirements
  - Replacement planning
- Asset Management
  - Asset inventory incl. security properties
- Risk Management
  - Risk Analysis (assessment & evaluation)
  - Risk Mitigation
- Lifecycle Management
  - Onboarding to EOL
  - Change mgmt., Maintenance (e.g. patching)
- Network Segmentation
  - Anomaly detection
  - Security Filters / Web Gateways
- Incident Response

Medical Device Cybersecurity

Evolution of the topic – sharing is caring

- ICS-CERT: Industrial Control System - Computer Emergency Response Teams (Homeland Security).
- Has been publishing medical device alerts since 2013.
- Steady increase in discovered & disclosed vulnerabilities.
- Depending on vulnerability and affected device population, impact may vary.
- Reported by security researchers and vendors.
- FDA Postmarket Guidance impact on Alerts:
  - 37 prior to guidance
  - 85 since guidance



Source - MedCrypt: “What Medical Device Vendors Can Learn From Past Cybersecurity Vulnerability Disclosures”

Health Technology ALLIANCE

Specific Concern: Medical Devices Security

Understanding and managing the risks

Patient Safety

- Intentional or unintentional incidents
- Reliability, functionality, availability
- Misdiagnosis, treatment errors

Privacy

- Information (PHI, PII, credentials)
- Data breach (transmission intercept, device loss or theft)
- Intellectual property (clinical trials & research)

Care Delivery

- Downtime due to equipment availability
- Impact on hospital operations
- Reduced ability to deliver care

Security

- Device used as means for intrusion – beachhead attack
- Impact on network performance, e.g. alarm delays
- DDoS (origin of or impacted by)

Business & Financial

- Reputation
- Revenue / Referrals
- Law suits / fines
- Stock value

Indirect Risks

- Patient trust
- Patient treatment decisions
- Staff morale
- National Security

Incidents reported to date: shutdown and impact on care delivery; devices exploited as “backdoor” for an attack.
Not reported to date: Patient or user harm (although there may have been unreported or unattributed cases).

Agenda

- Medical Device Cybersecurity – Why and Why Now?
- Special Issues Affecting Cybersecurity of Medical Devices
- Managing Medical Devices Cybersecurity Risks
- Overview of Resources

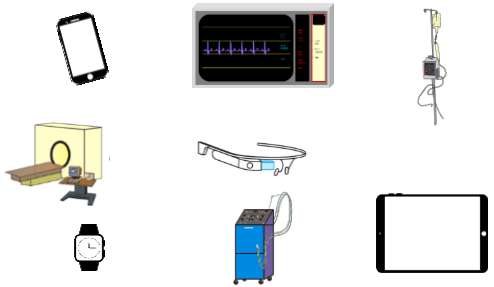
Special Issues with Medical Devices

- As many as 4 in 10 medical devices are networked or networkable
- Still more medical devices are firmware- or software-based … and can be accessed & compromised via non-network connections (e.g., via USB)
- Medical devices outnumber IT devices by 5 to 1 in most hospitals
- Medical devices are often overlooked or, at least, inadequately considered by security professionals who are better versed in information technology systems

Special Issues with Medical Devices

Medical Devices & Systems:

~ 10 Million in U.S. Hospitals today



Exponential growth of medical devices (including consumer platforms & wearables running medical applications) in hospitals, clinics, medical offices, workplace, schools, homes, etc.

You can't manage what you can't measure

Health Technology ALLIANCE

Special Issues with Medical Devices

~ 10 to 15 medical devices per bed

typical 500 bed hospital may have 7,500 medical devices

Examples of networked medical equipment types:

- Physiologic monitors ..... *hundreds*
- Defibrillators ..... *scores*
- Infusion pumps ..... *thousands*
- Anesthesia units ..... *scores*
- Ventilators ..... *scores*
- Extracorporeal Assist ..... *up to dozen*
- Vital sign monitors ..... *hundreds*
- CT & MRI scanners ..... *up to score*
- Fetal monitors ..... *scores*
- Laboratory analyzers ..... *scores*
- Diagnostic ultrasound ..... *scores*
- Patient beds ..... *hundreds*
- Electrocardiographs ..... *scores*
- Injectors, contrast media ..... *scores*

Health Technology ALLIANCE

Special Issues with Medical Devices

> 5% are considered Critical (i.e., can compromise can result in death or serious injury)

Examples of data that is subject to compromise:

- images from x-ray, CT, MRI, ultrasound,
- waveforms from ecg, bp, eeg
- demographic information …. e.g., personally identifiable information (PII)
- vital signs (e.g., heart rate, BP, pulse ox, resp, temp)
- alarm parameters
- drug type & dosage
- control and configuration settings (e.g., infusion rates, therapy timers, anesthesia & radiation delivery settings)
- laboratory (e.g., chemistry) results
- sounds from blood flow, respiration

Special Issues with Medical Devices

Common Types of Network Connections

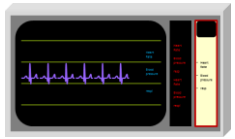
Types of connections via wired or wireless networks:

- Connect to electronic medical record (EMR)
- Connect to image/data storage (e.g., PACS)
- Remote access to data/images (e.g., physician, clinicians)
- Remote service (e.g., manufacturer updates, troubleshooting, repair)
- Remote management (e.g., clinical updates like drug libraries for infusion pumps)
- Remote control (e.g., modify alarms, configuration settings, level of therapy)
- Intra-communication between medical devices (e.g., diagnostic device “informing” therapeutic devices …. e.g., monitor controlling opioid delivery)

Special Issues with Medical Devices

Medical Devices and Systems: *Differences in Impact of Failure*

INFORMATION TECHNOLOGY



MEDICAL TECHNOLOGY

Security (i.e., data confidentiality, integrity or availability) compromise can

- ✓ *have serious financial impact*
- ✓ *have serious operational impact*
- ✓ *have serious reputation & legal impact*

Security compromise ***of Medical Device*** *can result in death or serious injury .*

Health Technology ALLIANCE

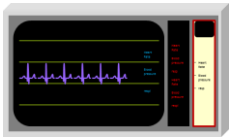
Special Issues with Medical Devices

Medical Devices and Systems: *Who has responsibility?*

IT knows data security

BUT …
IT generally has limited knowledge of type, number and vulnerabilities associated with medical devices

INFORMATION TECHNOLOGY



CE knows number/location of medical devices & understands criticality, lifecycle, and supportability issues

BUT …
CE generally has limited knowledge of data security issues

CLINICAL / BIOMEDICAL ENGINEERING
(HEALTHCARE TECHNOLOGY MANAGEMENT)

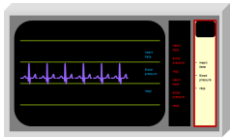
Health Technology ALLIANCE

Special Issues with Medical Devices

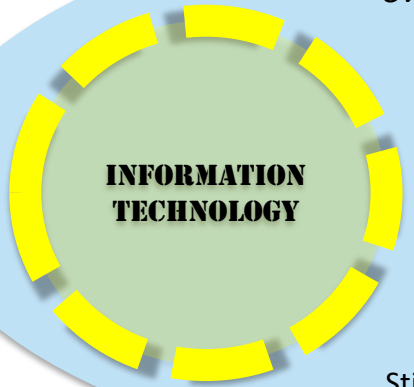
Medical Devices & Systems: Degree of Integrated Support

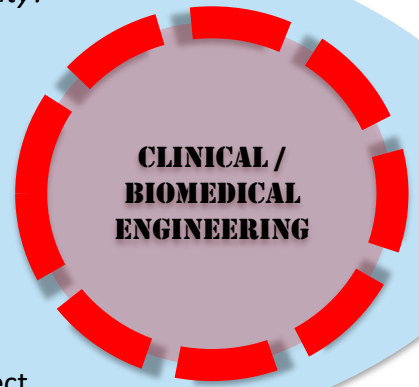
Currently 40%
Networked
(and rapidly growing)

Systems of Systems



Overlapping Responsibility?





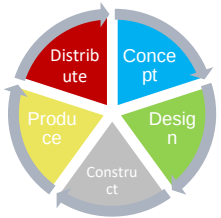
Still significant disconnect
… resulting in coverage gaps

Health Technology ALLIANCE

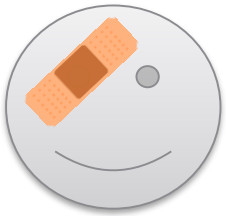
Special Issues with Medical Devices

Medical Devices & Systems: Differences in Development, Updates, Management

- As it currently stands, medical devices typically have a **7-8 year *product development cycle***
  - ✓ features including OS & software are “baked” in years before product release … and often years after consumer equivalent of software and hardware has moved to next generation
- Medical devices generally cannot be safely patched with OS updates or have virus software applied until patches have been specifically tested & approved by the device manufacturer
- Medical devices cannot have agents (e.g., SNMP) installed to facilitate network management



7-8 year
Product Life Cycle



Software update patches
& antivirus

Management
agents

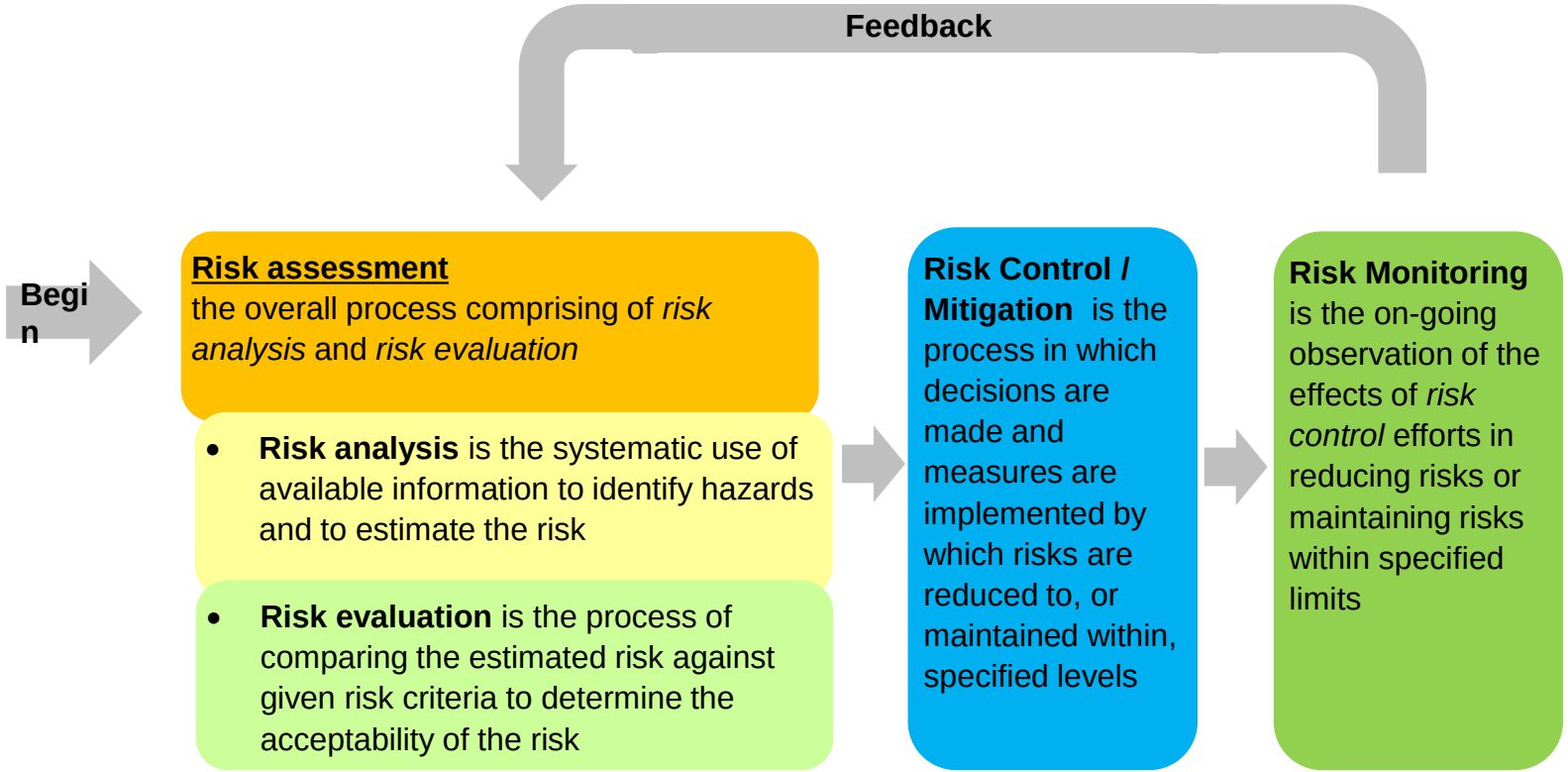
Health Technology ALLIANCE

Agenda

- Medical Device Cybersecurity – Why and Why Now?
- Special Issues Affecting Cybersecurity of Medical Devices
- Managing Medical Devices Cybersecurity Risks
- Overview of Resources

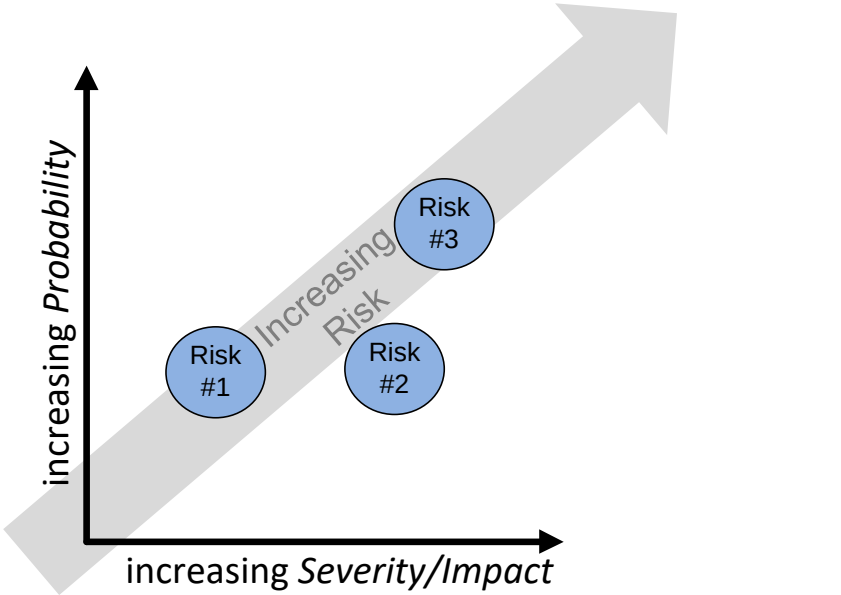
Managing Medical Device Cybersecurity Risks

Iterative Process



Generic Definition of Risk

Risk = Function (Severity/Impact, Probability)

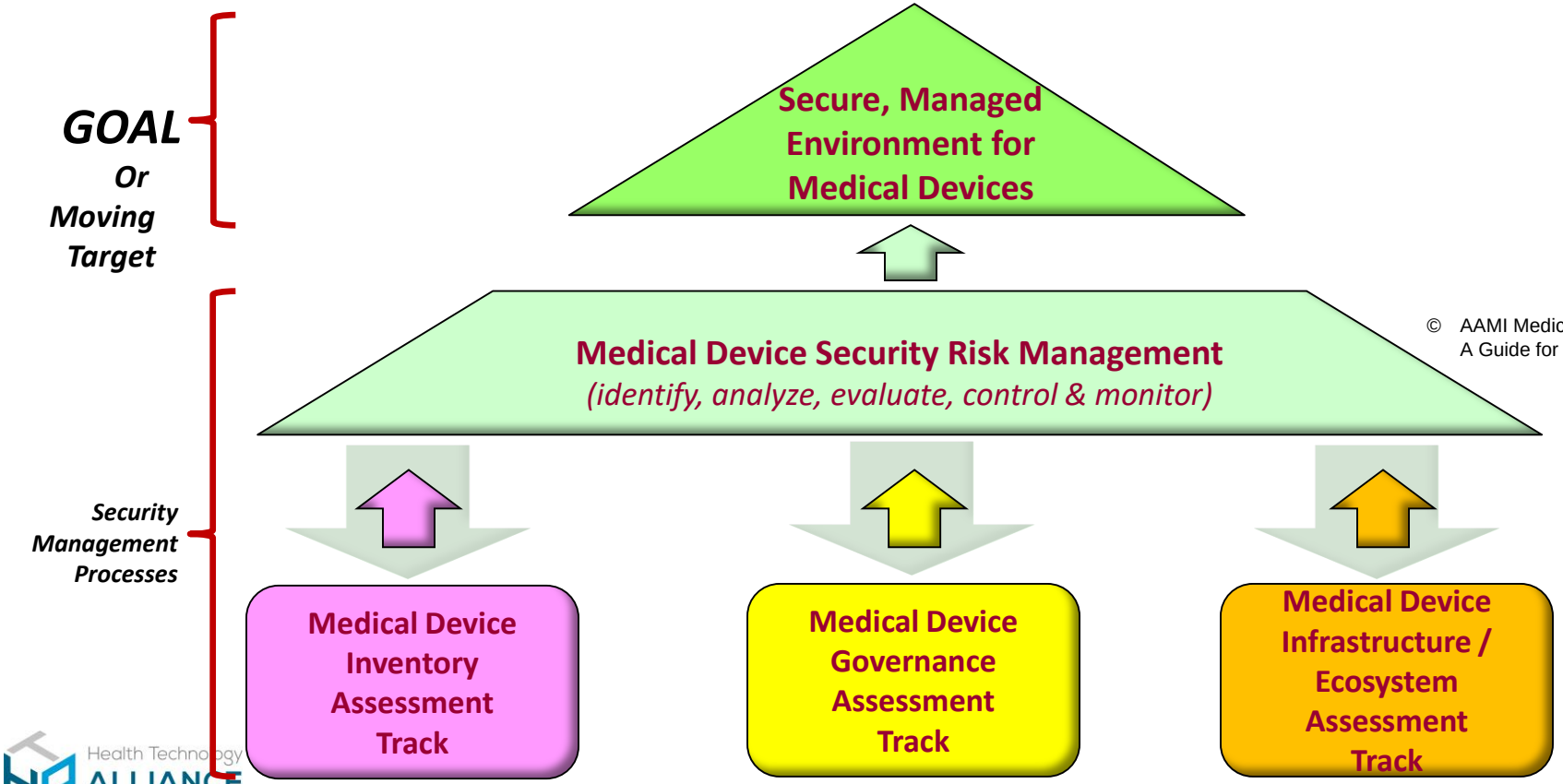


Risk Matrix for Determining Relative Risk Level

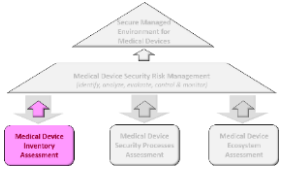
Risk Scoring

		Severity of Harm (Consequence)			
		1 Negligible	2 Marginal	3 Critical	4 Catastrophic
Probability of Harm	4 Probable	4	8	12	16
	3 Occasional	3	6	9	12
	2 Remote	2	4	6	8
	1 Improbable	1	2	3	4

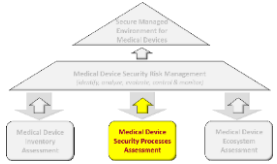
Managing Medical Device Cybersecurity Risks



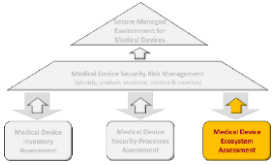
Processes for Managing Medical Device Cybersecurity Risks



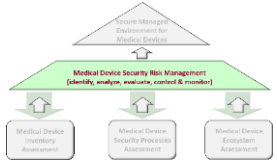
Track 1: Inventory



Track 2: Governance



Track 3: Ecosystem/Infrastructure



Risk Management

Health Technology ALLIANCE

TRACK 1

Medical Device Inventory

Start inventory

Ensure complete and accurate inventory of medical equipment

Is equipment controlled by or otherwise operated by firmware / software?

- Yes → In inventory, enter "yes" in "security issues?" field
- No → In inventory, enter "no" in "security issues?" field → End for this device

From manufacturer, obtain:
- MDS² (including security features, vulnerabilities)
- Mfg residual risk file
- software/firmware bill of materials (SBoM)
  - operating systems (version)
  - applications (version)
  - commercial-of-the-shelf software (COTS)
- Mfg recommendations for security config

Does equipment transmit or store PHI?

- Yes → In inventory, enter "yes" in "confidential data?" field
- No → In inventory, enter "no" in "confidential data?" field

Is equipment "connected" (i.e., connect via wire or wireless to other devices/systems)?

- Yes → In inventory, enter "yes" in "connected?" field
- No → In inventory, "no" in "connected?" field

Determine (and document in CMMS/CDMS) existing **configuration** info
- MAC, IP addresses
- types of connections
  - peer-peer, parent-child, client-server
  - network (e.g., VPN, wired or wireless ethernet, Bluetooth, etc.)
- type of encryption for data in-transit

Determine (and document in *device security risk management profile*):
- numbers & locations of these devices
- critical device functions
- types of data stored/transmitted
- type of encryption for data at-rest
- redundant/backup resources

TRACK 2

Medical Device Security Governance

Start Governance Review

Determine whether the organization has medical device security practices, policies & education (that, along with technical safeguards, provide defense-in-depth and that dovetail with relevant IT policies) related to:
- access management
  - role-based
  - passwords, keys
- encryption (data-at-rest, data-in-transit)
- change management
- life cycle management
  - acquisition / procurement
  - on-boarding (deployment, integration)
  - operation
  - support/maintenance (including patch management)
  - disposal / sanitization
- incident response that processes for
  - training
  - discovery
  - minimizing effects
  - reporting to appropriate groups & agencies
  - recovery
  - analysis
  - further evolution of mitigation & response

Determine whether the organization has access to appropriate resources and whether there are appropriate assignments & agreements with requisite stakeholders detailing their security responsibilities associated with:
- executive leadership support
- clinician (operator) support
- IT (e.g., network management, information security) support (including 3rd parties)
- HTM service support (including 3rd parties)
- manufacturer support
- materials management support
- risk management support
- business associates with access to PHI

TRACK 3

Medical Device Ecosystem

Start Infrastructure Review

Identify & document/map major elements of the organization's medical device infrastructure including:
- configuration management
- end point management
- architecture / isolated networks / VPN (wired/wireless)
- encryption (data-at-rest, data-in-transit), code obfuscation
- network discovery tool to find network elements and their configurations
- pen (penetration) testing to find network vulnerabilities
- traffic monitoring to identify anomalies (malware & peformance)
- anti-malware, whitelists, sandboxing
- remote access (applications, maintenance/support)
- compensating controls
- catalog of current relevant regulations, standards and best practices (e.g., AAMI, NIST, UL, FDA, ECRI, MITRE, etc.)
- established relationships with
  - information sharing and analysis centers/organizations (ISAC/ISAO) that collect and share vulnerability reports and mitigation guideance
  - US-CERT / ICS-CERT that publish alerts, bulletins, tips, technical documents
  - InfraGard .. providing a working partnership between FBI & private sector to report discovered threats, vulnerabilities and to provide guidance in addressing them

Risk Management

Assess (and score) ***severity*** of consequence (considering patient safety, patient care, operations, finance, or reputation) if
- **confidentiality** of PHI is compromised
- **integrity** or **availability** of any data is compromised

After identifying threats & vulnerabilites, Assess (and score) ***probability*** *(i.e., likelihood)* of data compromise related to
- confidentiality
- integrity or availability

Assess (and score) ***impact*** *(i.e., # of devices potentially affected)* of data compromise related to
- confidentiality
- integrity or availability

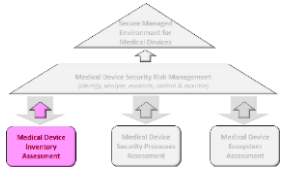
Determine security ***Risk*** associated with device
- confidentiality
- integrity or availability

where
Risk = Function (*severity/impact, probability*)

Control/treat identified risks by establishing mitigation plan (i.e., determine priorities, actions, schedules, assignments) based on security risk assessment. Risk treatment may include some combination of:
- risk transfer (e.g., insurance)
- risk reduction
  - ✓ administrative safeguards, *for example*
    - policies
    - education & training
    - etc
  - ✓ technical safeguards, *for example*
    - encryption
    - VPN, segregation
    - anti-malware
  - ✓ physical safeguards, *for example*
    - locks
    - etc
- risk acceptance

On-going monitoring, analysis, modification and review of security program processes, resources, and infrastructure [i.e., closed loop involving *input, process, result* & *feedback modifying input*]

Assessing Medical Device Cybersecurity Risks : Inventory (1 of 2)



Start Medical Device Inventory

Ensure complete and accurate inventory of medical equipment

Is equipment controlled by or otherwise operated by firmware / software?

- Yes → In inventory, enter "yes" in "security issues?" field
- No → In inventory, enter "no" in "security issues?" field → End for this device

From manufacturer, obtain:

- MDS^2 (including security features, vulnerabilities)
- Mfg residual risk file
- software/firmware bill of materials (SBoM)
  - operating systems (version)
  - applications (version)
  - commercial-of-the-shelf software (COTS)
- Mfg recommendations for security config

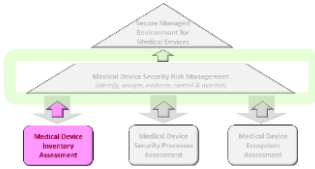
Does equipment transmit or store PHI?

- Yes → In inventory, enter "yes" in "confidential data?" field
- No → In inventory, enter "no" in "confidential data?" field

2

Health Technology ALLIANCE

Assessing Medical Device Cybersecurity Risks : Inventory (2 of 2)



1

Is equipment "connected" (i.e., connect via wire or wireless to other devices/systems) ?

Yes

In inventory, enter "yes" in "connected?" field

No

In inventory, "no" in "connected?" field

Determine (and document in CMMS/CDMS) existing **configuration** info

- MAC, IP addresses
- types of connections
  - peer-peer, parent-child, client-server
  - network (e.g., VPN, wired or wireless ethernet, Bluetooth, etc.)
- type of encryption for data in-transit

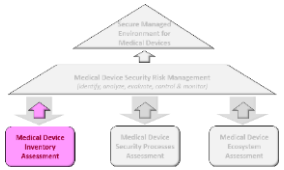
Determine (and document in *device security risk management profile*):

- numbers & locations of these devices
- critical device functions
- types of data stored/transmitted
- type of encryption for data at-rest
- redundant/backup resources

Risk Management Process

Typical Device Assessment (start with MDS2)

Examples of device inventory information



- Is device is software/microprocessor based?
- Does device connect to network, internet or other devices (wired or wireless)?
- Does device contains PHI?
- Have current versions of software/firmware been applied to device? (e.g., have available patches/updates been applied to device?)
- Has device been configured to disable unnecessary features
  - ✓ Hardware ports (e.g., USB) ?
  - ✓ Software ports ?
- Is data encryption at rest (stored in device) or transmitted sent/received by device?
- Is device physically accessible to other than patient and authorized (trained) users?
- Can device backup configuration and diagnostic/therapeutic data?

Assessing Medical Device Cybersecurity Risks: Governance (1 of 2)

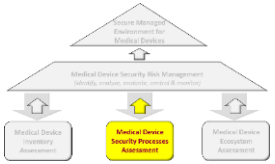
Measure to Manage

Fill the Process Gaps

Start Medical Device Security Processes

Determine whether the organization has medical device security practices, policies & education (that, along with technical safeguards, provide defense-in-depth and that dovetail with relevant IT policies) related to:

- access management
  - role-based
  - passwords, keys
- encryption (data-at-rest, data-in-transit)
- change management
- life cycle management
  - acquisition / procurement
  - on-boarding (deployment, integration)
  - operation
  - support/maintenance (including patch management)
  - disposal / sanitization
- incident response that processes for
  - training
  - discovery
  - minimizing effects
  - reporting to appropriate groups & agencies
  - recovery
  - analysis
  - further evolution of mitigation & response



Health Technology ALLIANCE

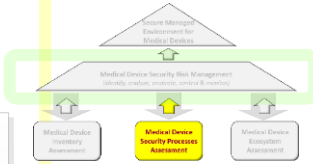
Assessing Medical Device Cybersecurity Risks: Governance (2 of 2)

1

Determine whether the organization has access to appropriate resources and whether there are appropriate assignments & agreements with requisite stakeholders detailing their security responsibilities associated with:

- executive leadership support
- clinician (operator) support
- IT (e.g., network management, information security) support (including 3rd parties)
- HTM service support (including 3rd parties)
- manufacturer support
- materials management support
- risk management support
- business associates with access to PHI

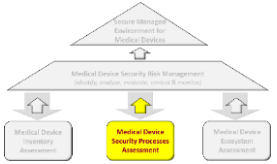
Risk Management Process



Governance Assessment

Examples of some medical device security practices, policies & education related to:

- “good hygiene” practices
- change management
- life-cycle management
  - ✓ acquisition / procurement
  - ✓ on-boarding (deployment, integration)
  - ✓ operation
  - ✓ support/maintenance (manufacturer engagement/ responsibility agreements including patch management)
  - ✓ disposal / sanitization
- incident response that processes for
  - ✓ training
  - ✓ discovery
  - ✓ minimizing effects
  - ✓ reporting to appropriate groups & agencies
  - ✓ recovery
  - ✓ analysis
  - ✓ further evolution of mitigation & response

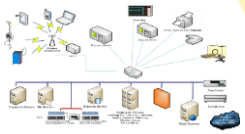


Assessing Medical Device Cybersecurity Risks: Infrastructure/Ecosystem (1 of 1)

Start Medical Device Infrastructure

Identify & document/map major elements of the organization's medical device infrastructure including:

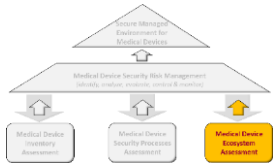
- configuration management including compensating controls
- end point management
- architecture / isolated networks (wired/wireless)
- encryption (data-at-rest, data-in-transit), code obfuscation
- network discovery tool to find network elements and their configurations
- pen (penetration) testing to find network vulnerabilities
- anti-malware, whitelists, sandboxing
- remote access (applications, maintenance/support)
- catalog of current relevant regulations, standards and best practices (e.g., AAMI, NIST, UL, FDA, ECRI, MITRE, etc.)
- established relationships with
  - information sharing and analysis centers/organizations (ISAC/ISAO) that collect and share vulnerability reports and mitigation guideance
  - US-CERT / ICS-CERT that publish alerts, bulletins, tips, technical documents
  - InfraGard .. providing a working partnership between FBI & private sector to report discovered threats, vulnerabilities and to provide guidance in addressing them



Risk Management Process

Ecosystem/Infrastructure Assessment

Examples of some Infrastructure / Ecosystem (i.e., outside-the-box) related approaches to medical device cybersecurity mitigation



- end point management
- architecture / isolated networks / VPN (wired/wireless)
- encryption (data-at-rest, data-in-transit), code obfuscation
- pen (penetration) testing to find network vulnerabilities
- traffic monitoring to identify anomalies (malware & performance)
- anti-malware, whitelists, sandboxing
- remote access (applications, maintenance/support)
- compensating controls

Preparing for Risk Control/Mitigation Following Risk Assessment

- Analyze *Inventory*, *Governance* and *Infrastructure/Ecosystem* and determine:
  - ✓ What are gaps (i.e., what are types of risks exist because assessment/analysis of inventory, governance, and infrastructure/ecosystem reveal inadequate precautions and what are gaps between existing and appropriate practices).
  - ✓ What are the relative levels of risks where risk=function(severity/impact, probability)
- Establish a control/mitigation plan by
  - ✓ Prioritizing plan for control/mitigation based on relative levels of risks determined
  - ✓ Determine appropriate steps to effectively control/mitigate known risks
  - ✓ Schedule/implement steps
  - ✓ Evaluate effectiveness

Fill the Process Gaps

Health Technology ALLIANCE

Medical Device Security Risk Management Process (1 of 2)

Medical Device Security Risk Management Processes

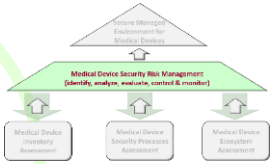
Assess (and score) ***severity*** of consequence (considering patient safety, patient care, operations, finance, or reputation) if
- **confidentiality** of PHI is compromised
- **integrity** or **availability** of any data is compromised

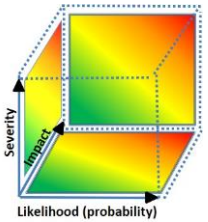
After identifying threats and vulnerbilities,
Assess (and score) ***probability*** *(i.e., likelihood)* of data compromise related to
- confidentiality
- integrity or availability

Assess (and score) ***impact*** *(i.e., # of devices potentially affected)* of data compromise related to
- confidentiality
- integrity or availability

Determine security ***Risk*** associated with device
- confidentiality
- integrity or availability

where
Risk = **Function** (*severity, impact, probability*)





Health Technology ALLIANCE

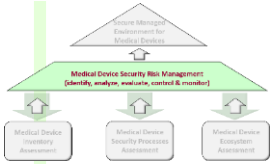
Medical Device Security Risk Management Process (2 of 2)

1

Control/treat identified risks by establishing mitigation plan (i.e., determine priorities, actions, schedules, assignments) based on security risk assessment. Risk treatment may include some combination of:

- risk transfer (e.g., insurance)
- risk reduction
  - ✓ administrative safeguards, *for example*
    - policies
    - education & training
    - etc
  - ✓ technical safeguards, *for example*
    - encryption
    - VPN, segregation
    - anti-malware
  - ✓ physical safeguards, *for example*
    - locks
    - etc
- risk acceptance

On-going monitoring, analysis, modification and review of security program processes, resources, and infrastructure [i.e., closed loop involving *input*, *process*, *result* & *feedback modifying input*]



(identify, analyze, evaluate, control & monitor)

Managing Medical Device Cybersecurity Risks

Examples of risk control/mitigation plan:

- The Risk Mitigation Worksheet

1	2	3	4	5	6	7	8	9	10
Device mfg/model, qty	Description of vulnerability (based on assessment)	Severity/Impact of potential compromise	Probability of potential compromise	Risk level (where Risk=function(severity/probability)	Proposed Control/Mitigation steps	Assignment	Schedule	Probability after Control/Mitigation complete	Risk after Control/Mitigation complete
xxxxxx	xxxxx	xxxxxxx	xxxxxx	xxxxx	xxxxxx	xxxxxx	xxxxxx	xxxxxx	xxxxxx

1. Device name, manufacturer, model, quantity
2. Description of vulnerability (based on assessment)
3. Severity/impact of potential device compromise
4. Probability of potential device compromise
5. Risk level (where risk=function[severity/probability])
6. Proposed control/mitigation steps
7. Assigned to
8. Schedule for control/mitigation complete
9. Probability after control/mitigation is complete
10. Risk after control/mitigation is complete

Health Technology ALLIANCE

Summary

- The introduction of *connected medical devices* are growing at nearly exponential rates in healthcare organizations
- Significant cultural and process gaps still exist between most those supporting traditional Information Technology (IT) and those clinical engineering (CE) / healthcare technology management (HTM) services supporting medical devices & systems
- Traditional data security measures are often not safe or appropriate for use on medical devices … special precautions must often be taken
- Healthcare organizations should be proactive and begin addressing medical device security by assessing the numbers and kinds of devices involved … and then evaluating the risks associated with the use of those devices

Agenda

- Medical Device Cybersecurity – Why and Why Now?
- Special Issues Affecting Cybersecurity of Medical Devices
- Managing Medical Devices Cybersecurity Risks
- Overview of Resources

Cybersecurity Fundamentals

Where to start?

Business Leadership

- Understand Cyber Risk as a Business Risk:
  - Board & Executive Leadership, Culture, Staffing & Budgets
- Establish Objectives:
  - Governance, Risk Tolerance, Security Strategy in Support of Technology Adoption (cloud, telehealth, etc.)
- Management and Decision Making:
  - Reporting, Auditing, Change Management, Status & Gap Reporting, Lessons Learned

Security Strategy

- Roles & Responsibilities:
  - IT, IS, Clinical Engineering, Facilities – and non-technical roles: Clinicians, Administration
- Relevant Regulations, Laws, Frameworks and Standards:
  - Risk Management, Cybersecurity, Privacy, Patient Safety
- Policies & Procedures:
  - Training, Risk Management, Security Controls, Asset and Data Classification

Security Tactics

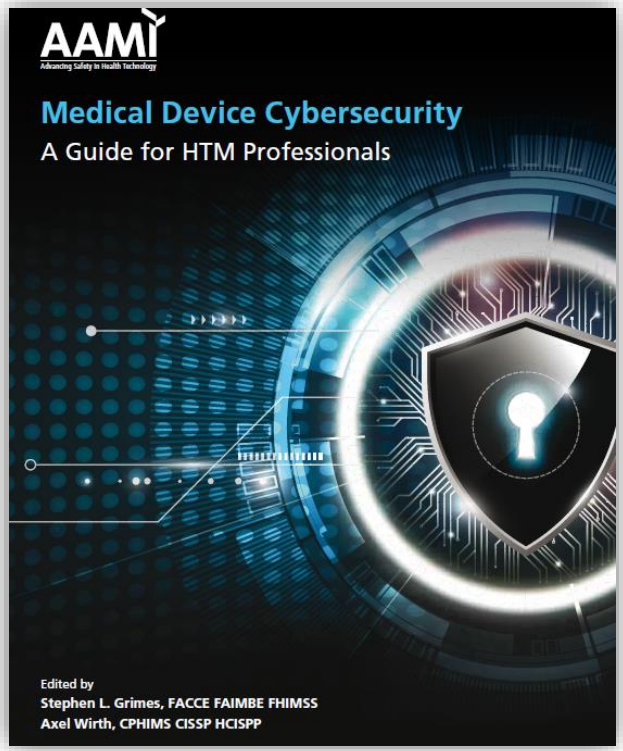
- Be able to Execute on Security Fundamentals:
  - Protect Device, Manage Device, Protect Network, Respond to Incidents
- Have Basic Housekeeping in Place:
  - Know you Assets, Prioritize, Manage Configurations (incl. patching), Segment Networks, Manage Vendors
- Security Operations:
  - Threat Intelligence, Security Mgmt., Identity Mgmt., Event Monitoring, Incident Response

AAMI Guide

Medical Device Cybersecurity: A Guide for HTM Professionals

Topics covered (on 248 pages)**:**

- Public Health Perspective
- Cybersecurity Fundamentals
- Patient Care Environment
- Technical Environment and Infrastructure
- Regulatory and Standards Environment
- Roles, Responsibilities,
- Inventory and Configuration Management
- Risk Assessment
- Risk Management
- Risk Mitigation
- Incident Response
- Trends and Future Developments
- Sample Procedures and Forms



http://my.aami.org/store/SearchResults.aspx?searchterm=MDC&searchoption=ALL

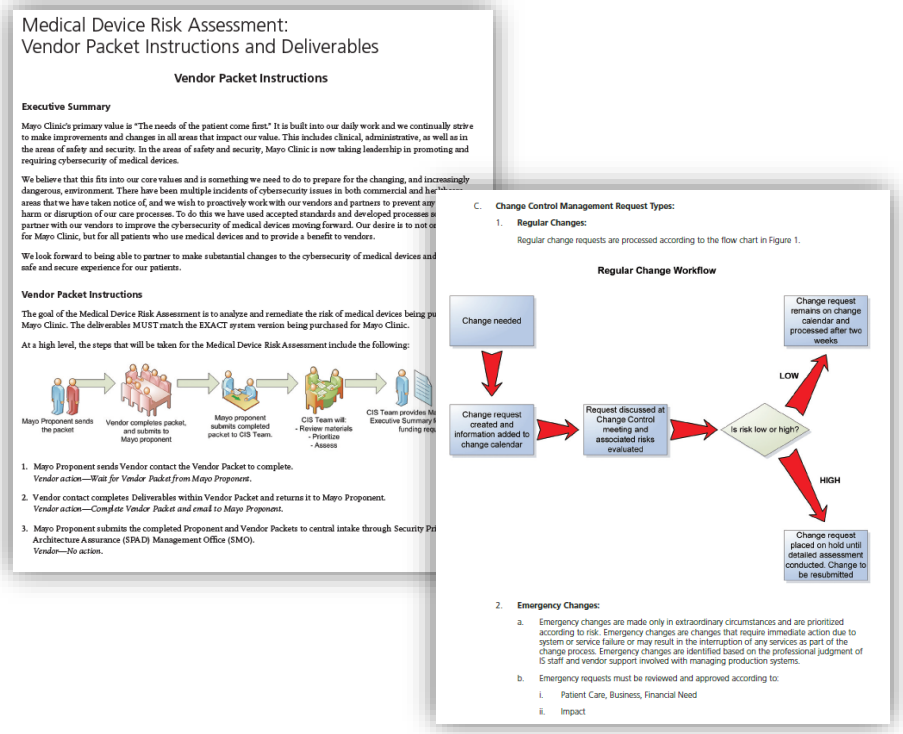
Health Technology ALLIANCE

AAMI Guide

Medical Device Cybersecurity: A Guide for HTM Professionals

Appendix:

- Terms & Definitions
- Acronyms
- Further Reading
- Cybersecurity Risk Management Flow Chart
- Example Tools, Policies, and Procedures:
  - Mayo Clinic
    - Vendor Packet Instructions and Deliverables
    - Technology and Security Requirements
  - Intermountain Health and Scripps Health
    - Change Management
    - Firewall Administration Change Control Policy
    - Lifecycle Ownership, Tracking, and Management
    - Disposal, Transfer, Reuse, and Data Sanitization
    - Operating System Vulnerability Management



Medical Device Risk Assessment:
Vendor Packet Instructions and Deliverables

Vendor Packet Instructions

Executive Summary

Mayo Clinic's primary value is "The needs of the patient come first." It is built into our daily work and we continually strive to make improvements and changes in all areas that impact our value. This includes clinical, administrative, as well as in the areas of safety and security. In the areas of safety and security, Mayo Clinic is now taking leadership in promoting and requiring cybersecurity of medical devices.

We believe that this fits into our core values and is something we need to do to prepare for the changing, and increasingly dangerous, environment. There have been multiple incidents of cybersecurity issues in both commercial and he areas that we have taken notice of, and we wish to proactively work with our vendors and partners to prevent any harm or disruption of our care processes. To do this we have used accepted standards and developed processes partner with our vendors to improve the cybersecurity of medical devices moving forward. Our desire is to not o for Mayo Clinic, but for all patients who use medical devices and to provide a benefit to vendors.

We look forward to being able to partner to make substantial changes to the cybersecurity of medical devices and safe and secure experience for our patients.

Vendor Packet Instructions

The goal of the Medical Device Risk Assessment is to analyze and remediate the risk of medical devices being pu Mayo Clinic. The deliverables MUST match the EXACT system version being purchased for Mayo Clinic.

At a high level, the steps that will be taken for the Medical Device Risk Assessment include the following:

Mayo Proponent sends the packet | Vendor completes packet, and submits to Mayo proponent | Mayo proponent submits completed packet to CIS Team. | CIS Team will: - Review materials - Prioritize - Assess | CIS Team provides Ma Executive Summary f funding req

1. Mayo Proponent sends Vendor contact the Vendor Packet to complete.
   Vendor action—Wait for Vendor Packet from Mayo Proponent.
2. Vendor contact completes Deliverables within Vendor Packet and returns it to Mayo Proponent.
   Vendor action—Complete Vendor Packet and email to Mayo Proponent.
3. Mayo Proponent submits the completed Proponent and Vendor Packets to central intake through Security Pr Architecture Assurance (SPAD) Management Office (SMO).
   Vendor—No action.

C. **Change Control Management Request Types:**

1. **Regular Changes:**

Regular change requests are processed according to the flow chart in Figure 1.

Regular Change Workflow

Change needed → Change request created and information added to change calendar → Request discussed at Change Control meeting and associated risks evaluated → Is risk low or high?

LOW → Change request remains on change calendar and processed after two weeks

HIGH → Change request placed on hold until detailed assessment conducted. Change to be resubmitted

2. **Emergency Changes:**

a. Emergency changes are made only in extraordinary circumstances and are prioritized according to risk. Emergency changes are changes that require immediate action due to system or service failure or may result in the interruption of any services as part of the change process. Emergency changes are identified based on the professional judgment of IS staff and vendor support involved with managing production systems.

b. Emergency requests must be reviewed and approved according to:

i. Patient Care, Business, Financial Need

ii. Impact

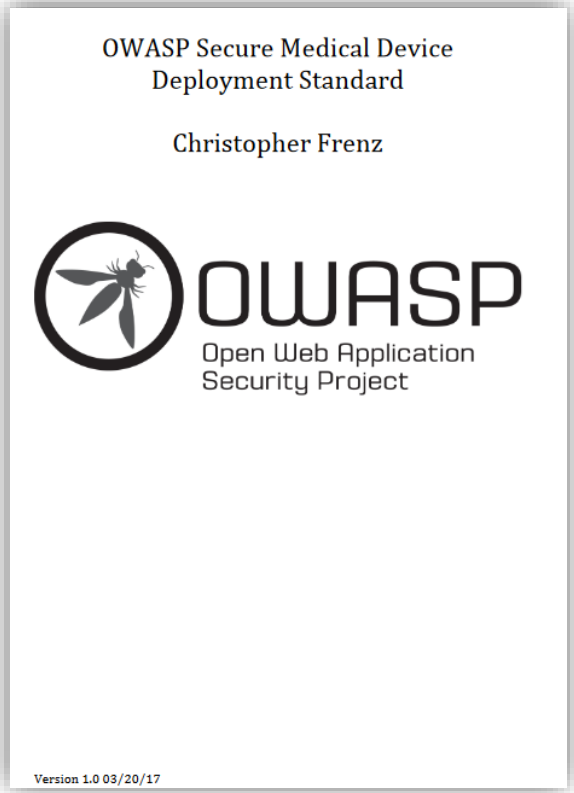
http://my.aami.org/store/SearchResults.aspx?searchterm=MDC&searchoption=ALL

Health Technology ALLIANCE

OWASP: Open Web Application Security Project

Secure Medical Device Deployment Standard, V1.0 03/20/17

- Purchasing Controls
  - Security Audit/Evaluation; Privacy Audit/Evaluation; Support
- Perimeter Defenses
  - Firewalls; Network Intrusion Detection System; Proxy Server/Web Filter
- Network Security Controls
  - Network Segmentation; Internal Network IDS; Syslog Server; Log Monitoring; Vulnerability Scanning; DNS Sinkholes
- Device Security Controls
  - Change Default Credentials; Account Lockout; Enable Secure Transport; Spare copy of firmware/software; Backup of device configuration; Baseline Configurations; Encrypt Storage; Different User Accounts; Restrict Access to Management Interface; Update Mechanisms; Compliance Monitoring; Physical Security; Asset Management
- Interface and Central Station Security
  - OS Hardening; Encrypted Transport; HL7 v3 Security Standards
- Security Testing
  - Penetration Testing
- Incident Response
  - Incident Response Plan; Mock Incidents



https://www.owasp.org/images/c/c3/SecureMedicalDeviceDeployment.pdf

IEC 80001 Series (HDO-focused)

Application of Risk Management for IT-Networks Incorporating Medical Devices

IEC 80001-1:2010 - “Part 1: Roles, responsibilities and activities”

IEC 80001-2-1:2012 - “Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples”

IEC 80001-2-2:2012 - “Part 2-2: Guidance for the communication of medical device security needs, risks and controls”

IEC 80001-2-3:2012 - “Part 2-3: Guidance for wireless networks”

IEC 80001-2-4:2012 - “Part 2-4: General implementation guidance for Healthcare Delivery Organizations”

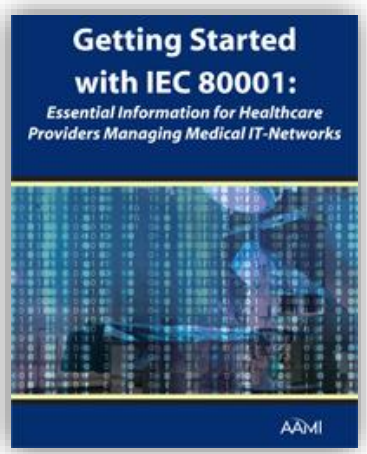
IEC 80001-2-5:2014 - “Part 2-5: Application guidance -- Guidance for distributed alarm systems”

IEC 80001-2-6:2014 - “Part 2-6: Application guidance -- Guidance for responsibility agreements”

IEC 80001-2-7:2015 - “Part 2-7: Application guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1”

IEC 80001-2-8 “Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2”

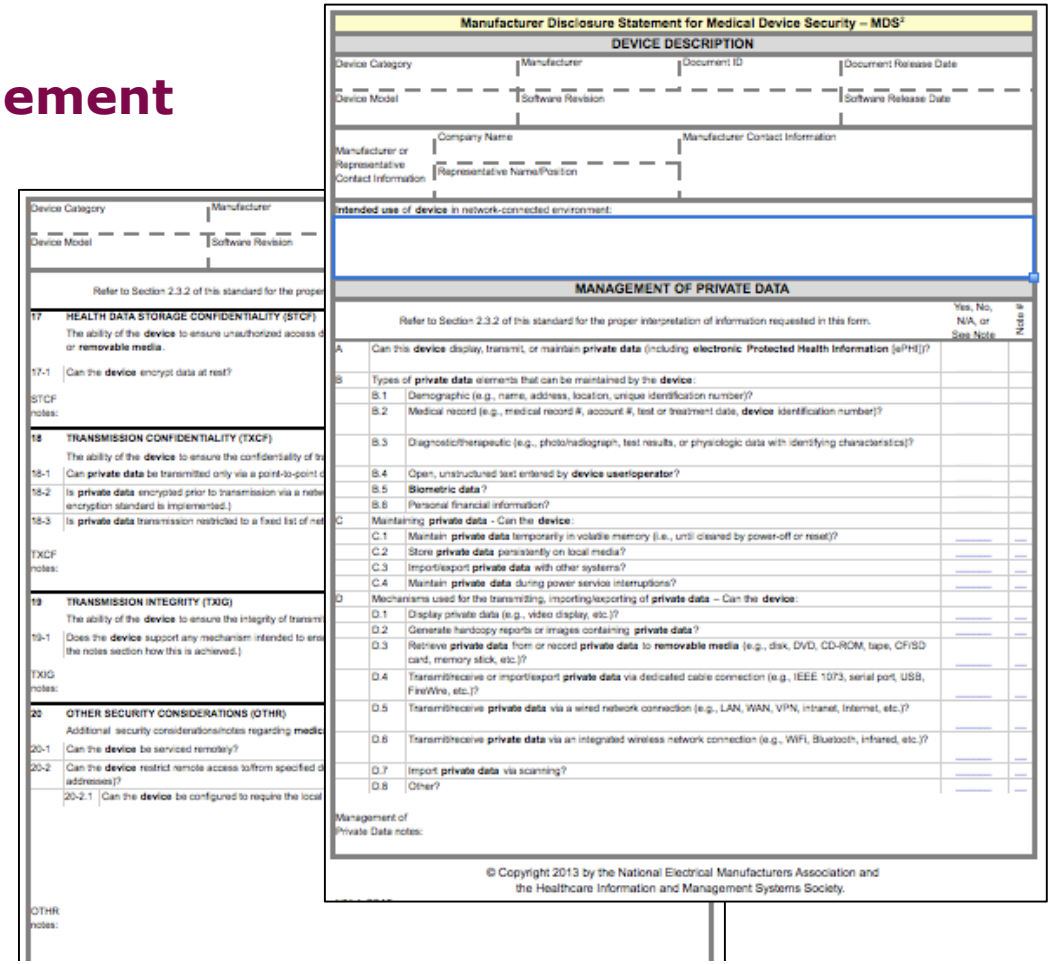
IEC 80001-2-9 “Part 2-9: Application guidance -- Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities”



Asset & Supply Chain Management

- Manufacturer Disclosure Statement for Medical Devices Security (MDS^2)
- Medical Device Security should be part of the Procurement Process:
  - RFP Language
  - Request NEMA MDS^2
- Developed in cooperation by HIMSS and NEMA

- Latest version Oct. 2013
- More detailed (2 -> 6 pages)
- Now harmonized with IEC 80001-2-2 technical controls
- New v3 currently being drafted



Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category | Manufacturer | Document ID | Document Release Date

Device Model | Software Revision | Software Release Date

Manufacturer or Representative Contact Information: Company Name | Representative Name/Position | Manufacturer Contact Information

Intended use of device in network-connected environment:

MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note #

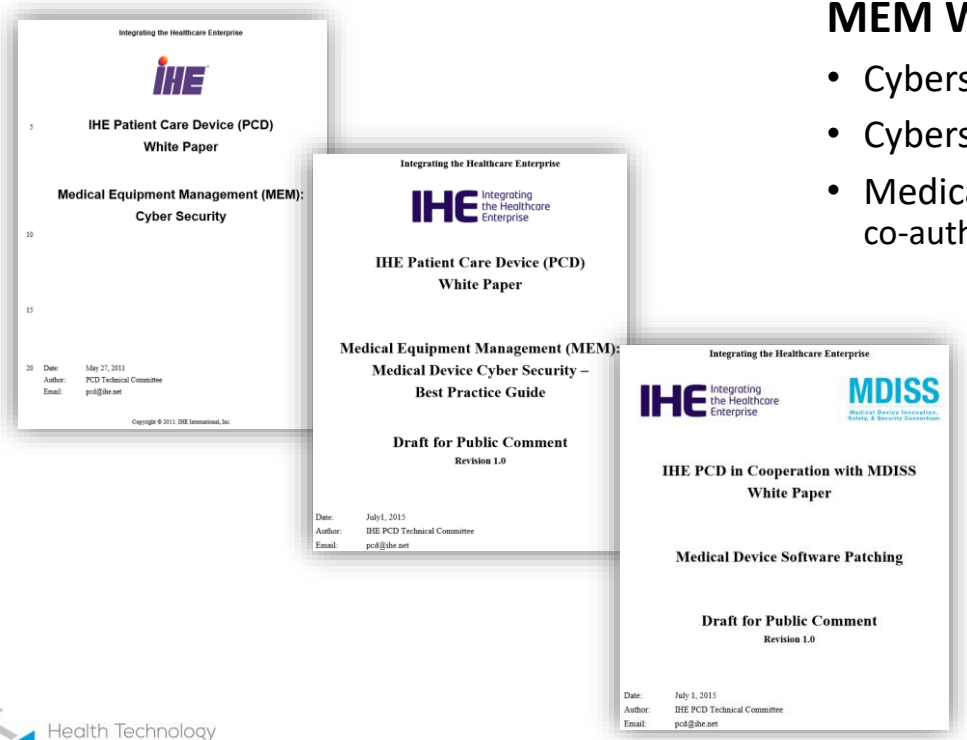
A	Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?	
B	Types of private data elements that can be maintained by the device:	
B.1	Demographic (e.g., name, address, location, unique identification number)?	
B.2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	
B.4	Open, unstructured text entered by device user/operator?	
B.5	Biometric data?	
B.6	Personal financial information?	
C	Maintaining private data - Can the device:	
C.1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?	
C.2	Store private data persistently on local media?	
C.3	Import/export private data with other systems?	
C.4	Maintain private data during power service interruptions?	
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device:	
D.1	Display private data (e.g., video display, etc.)?	
D.2	Generate hardcopy reports or images containing private data?	
D.3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	
D.4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	
D.5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	
D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	
D.7	Import private data via scanning?	
D.8	Other?	

Management of Private Data notes:

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

IHE International - PCD MEM

Patient Care Device Domain, Medical Equipment Management



MEM Whitepapers:

- Cybersecurity (2011: Education & Problem Baseline)
- Cybersecurity Best Practices (2015)
- Medical Device Patching (2015)
  co-authored by MDISS and IHE

Health Technology ALLIANCE

IEEE: Building Code for Medical Device Software Security

- Nov. 2014 Workshop
- Released May 2015
- Addressing device manufacturers' secure SW design needs.
- Key Elements:
  - Avoid vulnerabilities
  - Cryptography
  - SW integrity
  - Impede attackers
  - Enable detection
  - Safe degradation
  - Restoration
  - Maintain operations
  - Support privacy

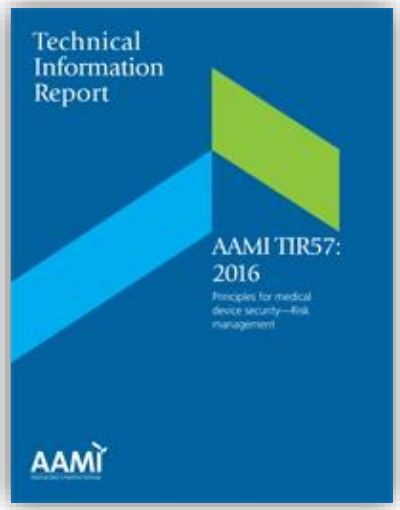
http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf

AAMI TIR57 (Manufacturer-focused)

Principles for Medical Device Security—Risk Management

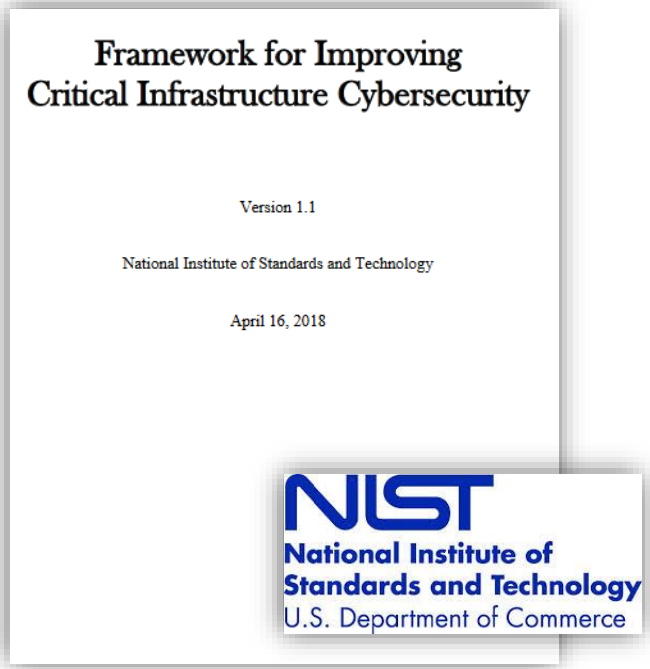
TIR 57 (technical information report) provides medical device manufacturers with guidance on developing a cybersecurity risk management process for their products:

- FDA-recognized standard
- Shows how to apply the principles of ANSI/AAMI/ISO 14971 (Medical devices—Application of risk management to medical devices) to security threats that could impact the confidentiality, integrity, and/or availability of medical devices.
- TIR57 lists six steps involved in the security risk management process:
  - Security risk analysis
  - Security risk evaluation
  - Security risk control
  - Evaluation of overall residual security risk acceptability
  - Security risk management report

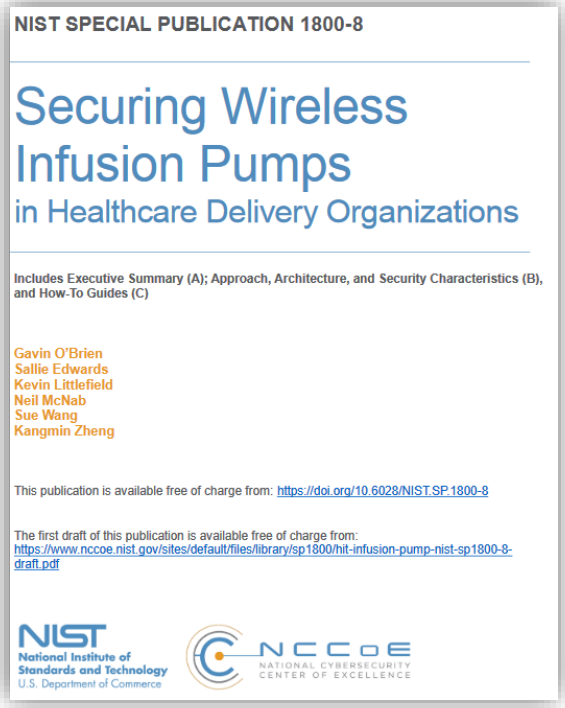


http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729

NIST Critical Infrastructure Cybersecurity Framework, National Cybersecurity Center of Excellence: NIST SP 1800-8



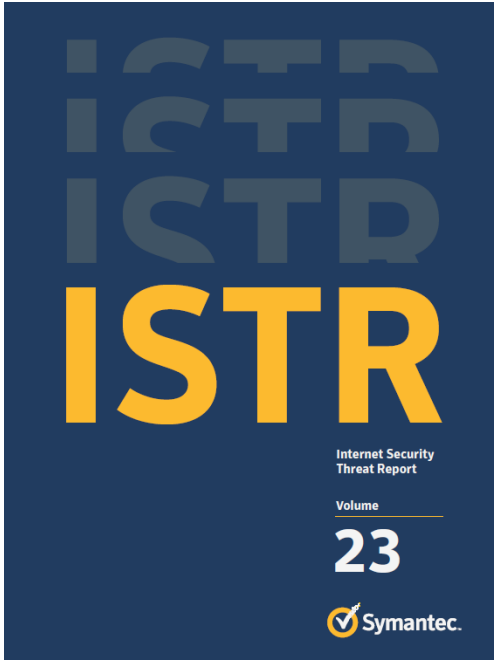
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf



https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf

Resources – Symantec

Further Resources via: www.Symantec.com/healthcare



https://www.symantec.com/security-center/threat-report

https://resource.elq.symantec.com/LP=5840?cid=70138000000rm1eAAA

Health Technology ALLIANCE

References - FDA

Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and FDA Administration Staff (Dec 2016)
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

Content of Premarket Submission for Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Administration Staff (Oct. 2014)
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software“ (updated July 2015)
http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.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

Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Jan. 2005)
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

Off-The-Shelf Software Use in Medical Devices (Sept. 1999)
http://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf

References - Other

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

References - Other

Manufacturer Disclosure Statement for Medical Device Security, NEMA (Oct. 2013); http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

UL 2900 Standards Process: Cybersecurity for Network-Connectable Products: https://industries.ul.com/cybersecurity/ul-2900-standards-process

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

MedCrypt: What Medical Device Vendors can learn from past Cybersecurity Vulnerability Disclosures https://www.medcrypt.co/medcrypt-vulnerability-analysis-whitepaper-1.pdf

“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/

Contact us

Stephen.Grimes@SHCTA.com Axel_Wirth@Symantec.com

Securing Medical Devices in your organization

The journey of a thousand miles begins with one step.

- Lao Tzu
6 Century BC

Health Technology ALLIANCE