CyberSecurity in Wireless Medical Devices

Bill Saltzstein

Code Blue Consulting

CyberSecurity Meetup: July 20 2017

Agenda

* Who am I, and how did I get here?
* Short-range wireless connectivity
* Cybersecurity Issues
* Q&A

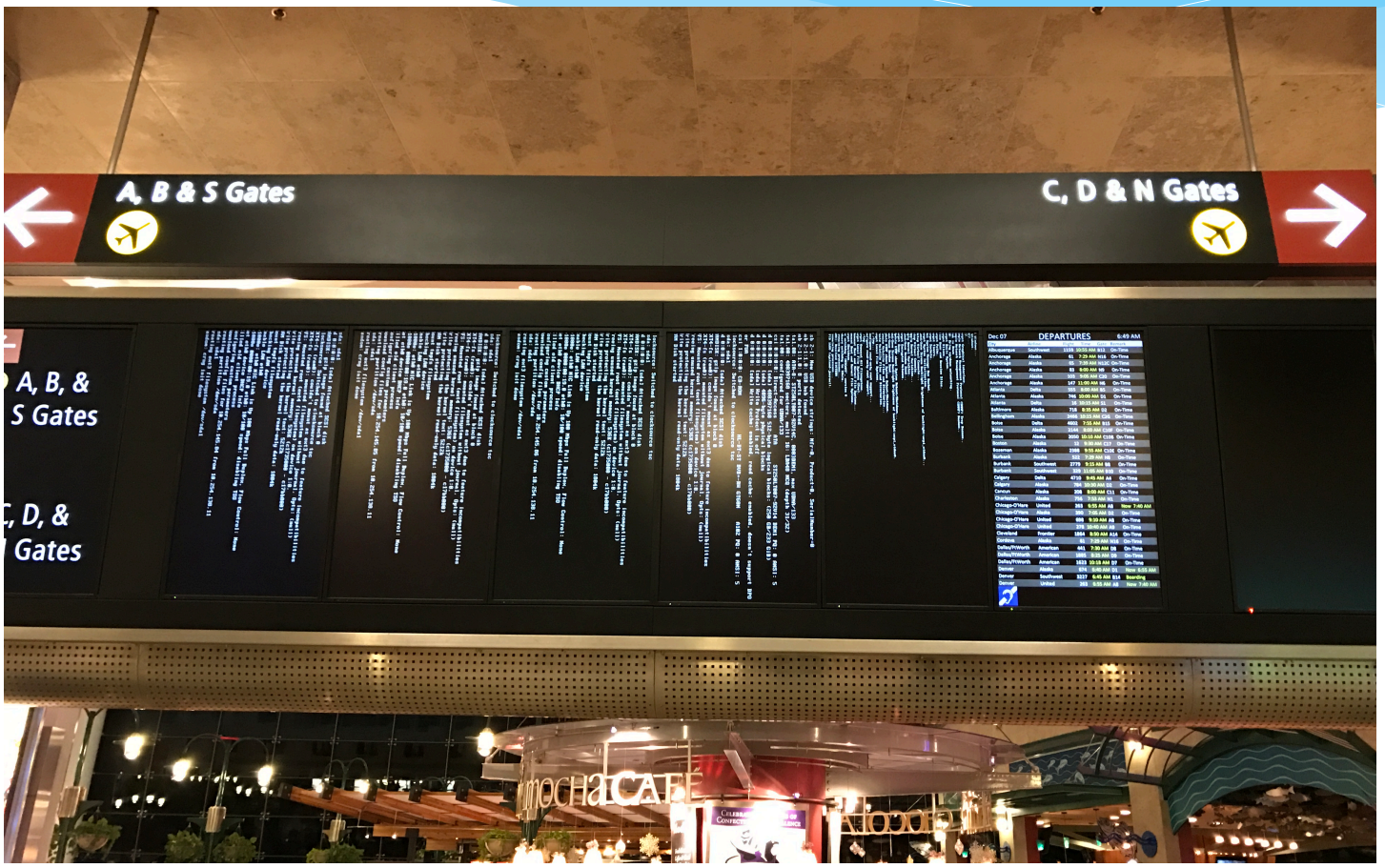
Who am I?

* EE, University of Rochester
* HP Calculators (HP-71B, HP-18/28)
* HP Cardiology (Pagewriter XL ECG, CodeMaster Defibrillator)
* Instromedix (LifeSigns Home Health)
* Medtronics Physio-Control (Dir. Adv. Dev.)
* Code Blue Communications (Bluetooth modules, consulting)
* connectBlue (Sales and Marketing)
* Code Blue Consulting & Cocoanut Manor (BTLE products)
* Cinq Cellars winery (gratuitous plug)

Consumer, Type I, II, III devices, 510(k), PMA, PMAs

Take the red pill, Neo

Think about this from a medical device…



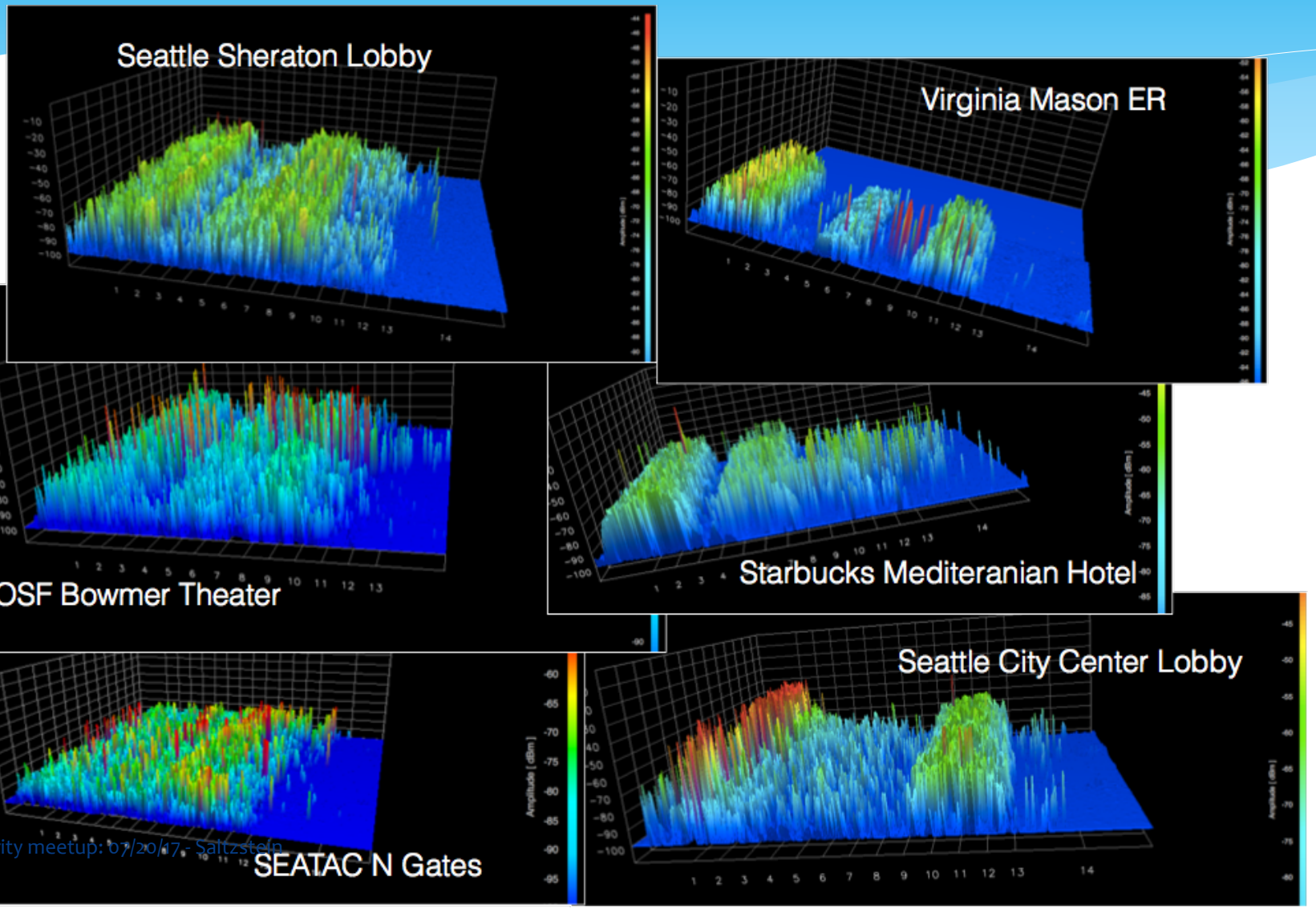
What is a Medical Device?

* A Medical Device is "… an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent.....", that is "...intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man..." or "...intended to affect the structure or any function of the body of man…" (from the US FDA)

The new MDDS & Medical Device and wireless technologies

- **WLAN**
  - **802.11b/g/n: 2.4 GHz, DSSS/OFDM**
  - **802.11a/n: 5.2 GHz, OFDM**
- **Bluetooth**
  - **Smart Ready: 2.0+EDR, low energy: 2.4 GHz, FHSS**
- **NFC**
  - **13.56 MHz**
- **A-GPS (rcv only)**
  - **L1: 1575.42 MHz**
  - **L2: 1227.6 MHz**
- **Glonass (rcv only)**
  - **L1: 1602 MHz (fc)**
  - **L2: 1246 MHz (fc)**
- **CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)**
- **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)**
- **TD-SCDMA 1900 (F), 2000 (A)**
- **GSM/EDGE (850, 900, 1800, 1900 MHz)**
- **FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)**
- **TD-LTE (Bands 38, 39, 40, 41)**

The 2.4 GHz world…



Demo

* WiFi Scanner – 802.11 at 2.4GHz and 5GHz
* Lightblue – Bluetooth low energy

Examples

* Hospital equipment
  * Defibrillator
  * Bedside patient monitor
  * MRI
  * Infusion pump
  * …
* Chronic disease management
  * Diabetes
  * Pulmonary: COPD
  * Heart disease
  * Pain

* Rx *delivery*
* Diagnostics out of hospital
  * External/wearable
  * Implanted
* Home Health
  * Infusion
  * Dialysis
  * Sleep apnea

All medical (and health) devices *shall* be connected

* Why?
* Where?
* How?

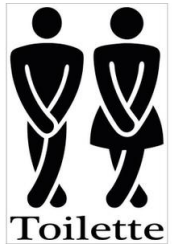
All medical devices *shall* be connected – Why?

* Connectivity
  * Electronic Health Record (EHR)
  * Charge capture (billing)
  * Big Data analytics
* Wireless is replacing wired connections
  * Mobility/safety
  * Data collection
* Telemedicine
  * Remote consultation & review (*photo*)
  * Home Health
  * Aging in Place
* Health and Fitness

Emergency!
1972-1977

All medical devices *shall* be connected – Where?

* Classic answers:
  * Hospital
  * EMS
  * Home
* Real answers:
  * Starbucks
  * 37,000 feet
  * Stuck on I-5
  * In the bathroom
  * In the elevator
* Real environments require creative solutions for connectivity



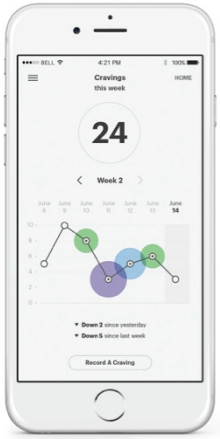
Example ***system***: Chrono Therapeutics

Wearable:
Sensors, button,
Rx delivery

Usage,
data

Settings,
software

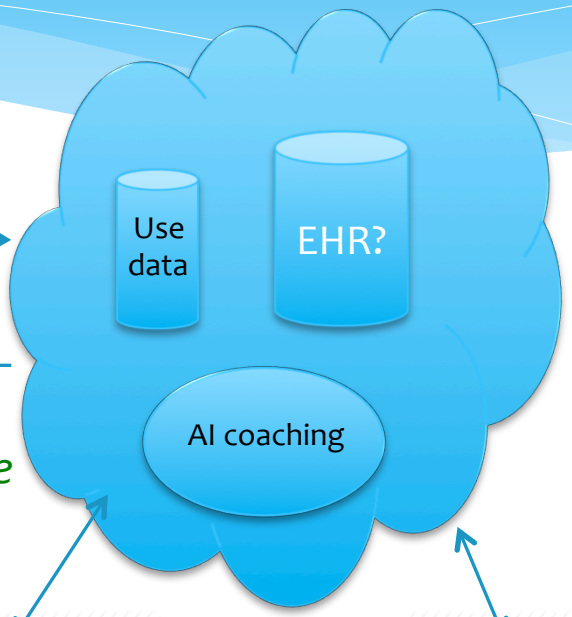
Short-range

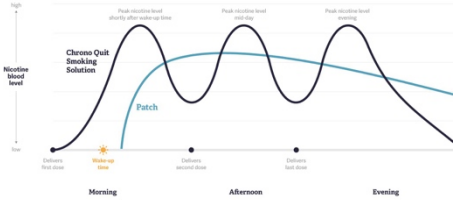


Patient info,
data

Settings,
software

Long-range





Real-time
Personal
Coaching/
Analytics

Enterprise

Billing

Photos and information obtained
from www.chronothera.com

Wandering and wondering in the wide world of short-range wireless

* Two real choices for short range data transfer
  1) WiFi – IEEE802.11
  2) Bluetooth
     a) Bluetooth classic
     b) Bluetooth low energy
* Everything else
  * RFID/NFC – expect usage in UDI and asset tracking
  * ZigBee, Thread – IEEE 802.15.4 based – coexistence challenge
  * MICS (Medical Implant Communication System) – supply, $$
  * MBAN (Medical Body Area Network) - ??

What are the issues for Medical Devices and networks?

* Medical Device data
  * Patient information (personal, medical)
    * “Protected Health Information” - PHI
  * Measurements and waveform
  * Device & network configuration and provisioning
  * Firmware upgrade
  * Security certificates
* The attack surface increases as connectivity increases

Why do we care?

* Patient lives are at stake, both directly and indirectly!
* HIPAA requirements – medical record portability & privacy
  * Protects you from unauthorized use of your medical information
  * Eg: employer discriminating for a medical condition
* FDA requirements
  * OTS software guidance
  * Premarket submission guidance
  * Postmarket management
* Company reputation and value is at stake
  * St Jude Medical/Muddy Waters

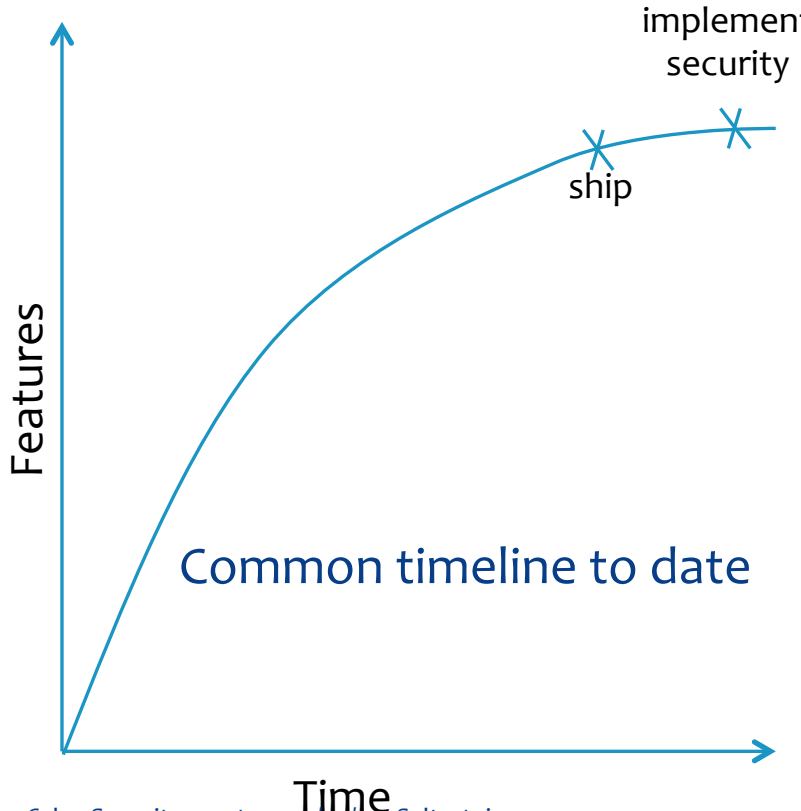
How real is this?
Hacking is evolving and accelerating!

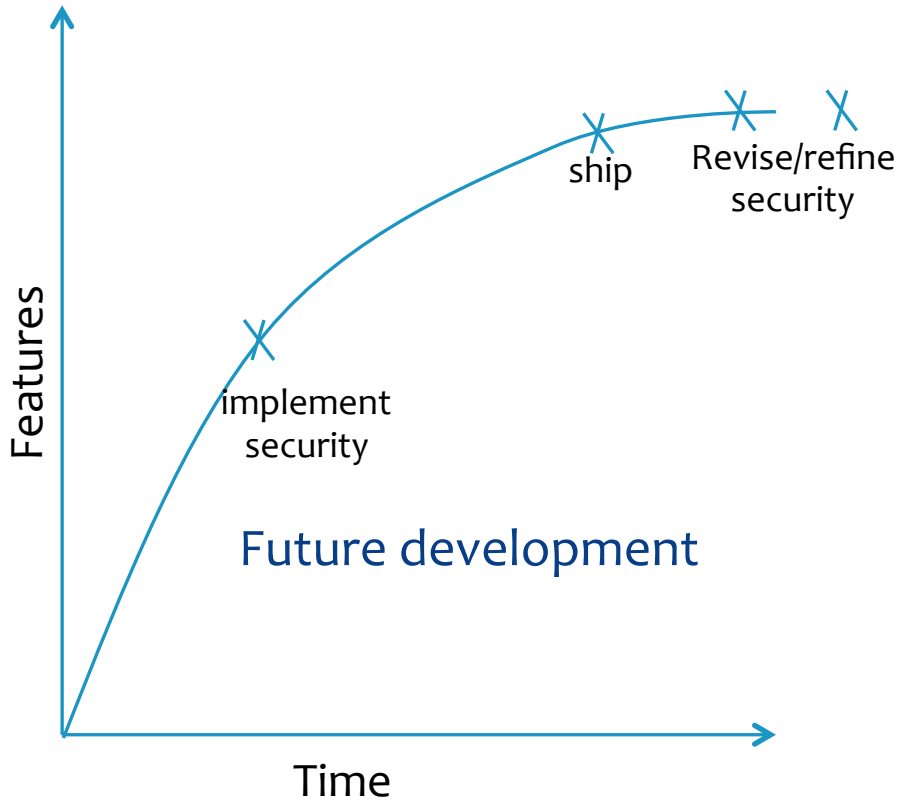
* Early public disclosure: "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses" - *2008 IEEE Symposium on Security and Privacy*
* 2015 - Hospira infusion pumps: *https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/*
* Recently: "Los Angeles Hospital Pays Hackers $17,000 After Attack" – February 2016
* Very recently: "J&J warns diabetic patients: Insulin pump vulnerable to hacking" – October, 2016
* Not medical, but very interesting: Segway Bluetooth hack: https://www.wired.com/story/segway-minipro-hack

IoM: the Internet of Medical

* Medical devices are IoT devices going forward
  * "Hacked Cameras, DVRs Powered Today's Massive Internet Outage", October 16, 2016
  * The 'botnet of things'?
* Ransomware, ex: WannaCry – May 2017, more than 230,000 computers in over 150 countries, lots of hospital computers included…
- Medical device designers need to design and implement *appropriate* cybersecurity measures

Why does this happen?
Development lifecycle & cybersecurity





Making security part of the Product Lifecycle

* Requirements
* Specifications
* Hazard analysis/Risk analysis and management
* Testing
* Release criteria
* Continuous monitoring & improvement
  * Monitoring
  * Update releases

Risks to consider - examples

* Modification of information Misuse of information
* Denial of use
* Open ports
* Unused/unnecessary profiles/services
* Unauthorized apps on system
* Debugging code or entries
* Off The Shelf (OTS) software patch doesn't get applied
* OTS software is changed without being validated
* Malware Endanger patient health Compromise identity or privacy

Potential wireless-specific hazards

* Eavesdropping
* Spoof/mimic data connections
* Man in The Middle (MTM) attacks during pairing
* Over The Air (OTA) upgrades
* Setting changes
* Advertising promiscuously

Regulatory guidance and requirements

* The FDA recently clarified guidance for software revisions due to cybersecurity
  * No agency submissions required
* NIST Cybersecurity Framework, Draft v1.1 - 1/17
* Recent US Government report: “Report on Improving Cybersecurity in the Health Care Industry”
* See references provided for specific guidance

My advice to clients

* Don't panic, but think like a hacker
* Apply *appropriate* measures relative to the risk
  * Consider usability
  * Consider patient safety – can not compromise!
* Make cybersecurity part of hazard analysis and mitigation process
* Consider end-to-end data path
* Follow & read up on news – this is an evolving issue
* Limit attack surface
* Consider connectivity changes that present new and unintended points of attack or disclosure

Q&A

* Bill Saltzstein
  Code Blue Consulting
  bill@consultcodeblue.com
  425-442-5854

Reference material

Recommended FDA guidance

* FDA landing page for Digital Health
  * http://www.fda.gov/medicaldevices/digitalhealth/
* General Wellness: Policy for Low Risk Devices
  * http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf
* Mobile Medical Applications
  * http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf
* Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices
  * http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM401996.pdf
* Radio Frequency Wireless Technology in Medical Devices
  * o http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf
* Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices
  * http://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf
* SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION (draft)
  * http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm524904.pdf
* Enforcement discretion
  * http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm

Selected Cybersecurity References

* Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
  * http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf
* Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
  * http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
* Postmarket Management of Cybersecurity in Medical Devices
  * http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
* ISO 14971:2007 Medical devices -- Application of risk management to medical devices
  * http://www.iso.org/iso/catalogue_detail?csnumber=38193
* HHS: Your Mobile Device and Health Information Privacy and Security
  * https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
* Archimedes – Ann Arbor Research Center for Medical Device Security
  * https://secure-medicine.org
* BITAG: Internet of Things (IoT) Security and Privacy Recommendations
  * http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
* Diabetes Technology Society: https://www.diabetestechnology.org/dtsec.shtml

AAMI

* TIR57: Principles for medical device security—Risk management
  * https://standards.aami.org/kws/public/projects/project/details?project_id=876
* TIR59: Risk Assessment of radio-frequency wireless coexistence for medical devices and systems
  * https://standards.aami.org/kws/public/projects/project/details?project_id=1114
  * AMSI C63.27
  * AAMI TIR69 as well for coexistence

NIST

* NIST: Cybersecurity Practice Guide, Special Publication 1800-1: "Securing Electronic Health Records on Mobile Devices”
  * https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices
* NIST: Guide to Bluetooth Security
  * http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf
* Cybersecurity Framework v1.1 – 1/17
  * https://www.nist.gov/cyberframework/draft-version-11
* Infusion pump draft
  * https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

Bluetooth SIG

* Transcoding (and other) Whitepapers: https://www.bluetooth.com/develop-with-bluetooth/white-papers