Secrets of successful medical device connectivity

Bill Saltzstein
Code Blue Communications
Playbook Vancouver 2017

* The secrets:
  * All medical devices shall be connected
  * You shall understand the requirements
  * Wandering and wondering the wide world of wireless
  * Two keys/pleas from me
  * Q&A

Agenda
All medical devices shall be connected

* Why?
* Where?
* How?

Replace wired connections
- Mobility/safety
- Data collection
- Telemedicine
  - Remote consultation & review (photo)
- Home Health
- Aging in Place
- Health and Fitness
- Cloud connectivity
  - Electronic Health Record (EHR)
  - Big Data analytics
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: Chrono Therapeutics Technology + Psychology

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.chronoothera.com
How: Understand the requirements requirements for connectivity

* Too many times we come up with the answer before the question (42)
* Connectivity doesn’t make the product
* Connectivity enables the product
* Behavior modification: Technology can not directly address Psychology
* Understanding the use model is essential for connectivity decisions
* Users – note the ‘s’
* Environment – home, Starbucks, hospital, EMS, airplane, …
* International
* Requirements to consider for mobility
* Power management and charging – batteries, batteries, batteries!
* Body proximity – antennas, antennas, antennas!
* BYOD (Bring Your Own Device)

Wandering and wondering in the wide world of wireless

* Two real choices for short range
  1) WiFi
  2) Bluetooth
* Multiple flavors of Cellular for long range (nG, low rate)
* Everything else
  * MICS (Medical Implant Communication System)
  * MBAN (Medical Body Area Network)
  * ZigBee, Thread (802.15.4)
* Heresy: remember that a wire can still be a good thing
* Remember to consider/compare the wired experience
How to choose?

* Go back to your requirements and environment!
  * If you need long-range, independent connectivity → cellular
  * If you’re in hospital and need EHR connectivity → WiFi
  * For anything else → Bluetooth
    * Full disclosure: I’m a Bluetooth geek…
  * Right, now which flavor of Bluetooth?
    * Bluetooth classic if
      * Audio
      * High-rate streaming
      * Long range
    * For now… Bluetooth 5 provides for those needs if you can wait

The dual-edge of standards

* The issues:
  * Is there real compatibility?
  * Marketplace – is compatibility an asset or a liability?
  * Regulatory and testing
  * Wireless standards bodies
    * Bluetooth SIG – legal requirement
    * WiFi Alliance – marketplace requirement!
  * Industry compatibility specifications
    * AAMI – primarily for in-hospital devices
    * Continua Alliance
    * Bluetooth SIG
      * Bluetooth Transcoding Whitepaper
    * Health/medical profiles – use them if you wish
    * With Bluetooth low energy you can make your own
  * Medical regulatory requirements
    * FDA
    * European regulations (and what about the UK?)
    * Other country-specific requirements
My pleas – Please!

* Design for regulatory
  * Understanding testing requirements
  * Real-world environment based
  * Interoperability/compatibility
  * Design-in testability features
* Design for security
  * Security as part of hazard analysis & mitigation
  * Don’t do this →

Summary

* The true secrets are in Understanding and Planning
* Understand where and how connectivity benefits/enables your system
* Understand the use models
* Pick the technology and system components based on the requirements, not the cool-factor
* Design-in for regulatory and security up front
Q&A

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

Backup slides and reference material
Notes on requirements

- Extract requirements, not solutions
  - Yes: “battery powered”, “disposable”, “body-worn using adhesive”, “interface to smartphones”
  - No: “Bluetooth low energy”
- Identify Interoperability and Compatibility
  - Medical device interoperability – how does it operate/interface to other systems or devices
  - Infrastructure - “shall connect using in-hospital wireless infrastructure”
  - Information systems – “shall support data flow to EHS including Cerner and McKesson”
- Identify Obsolescence and technology life cycle
  - Consider mismatch between Medical Device lifecycle and Wireless technology lifecycle
  - “shall be maintained for 5 years of sales, 10 years of support”
- Consider CyberSecurity
  - “shall comply with HIPAA”
  - “shall support US VA sales” (eg: FIPS 140-2 specification requirement)
- Identify Country-specific regulatory requirements
  - “shall support sales to the following countries”
  - Good to include these in groups – initial countries, 2nd wave, 3rd wave, …

Recommended FDA guidance

- FDA landing page for Digital Health
  - http://www.fda.gov/medicaldevices/digitalhealth/
- General Wellness: Policy for Low Risk Devices
- Mobile Medical Applications
- Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices
- Radio Frequency Wireless Technology in Medical Devices
- Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices
- SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION (draft)
- 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
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Postmarket Management of Cybersecurity in Medical Devices
  - https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices
- NIST: Guide to Bluetooth Security
- ISO 14971:2007 Medical devices -- Application of risk management to medical devices
- HHS: 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

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

The 2.4 GHz world...