MEDICAL DEVICE SYSTEMS AND BLUETOOTH® WIRELESS TECHNOLOGY: OPPORTUNITIES AND CHALLENGES

Making Medical Devices Wireless in the Digital Health Age: Issues, Risks, and Practical Advice

Bill Saltzstein
Code Blue Consulting

Bluetooth®

Code Blue Consulting

Outline

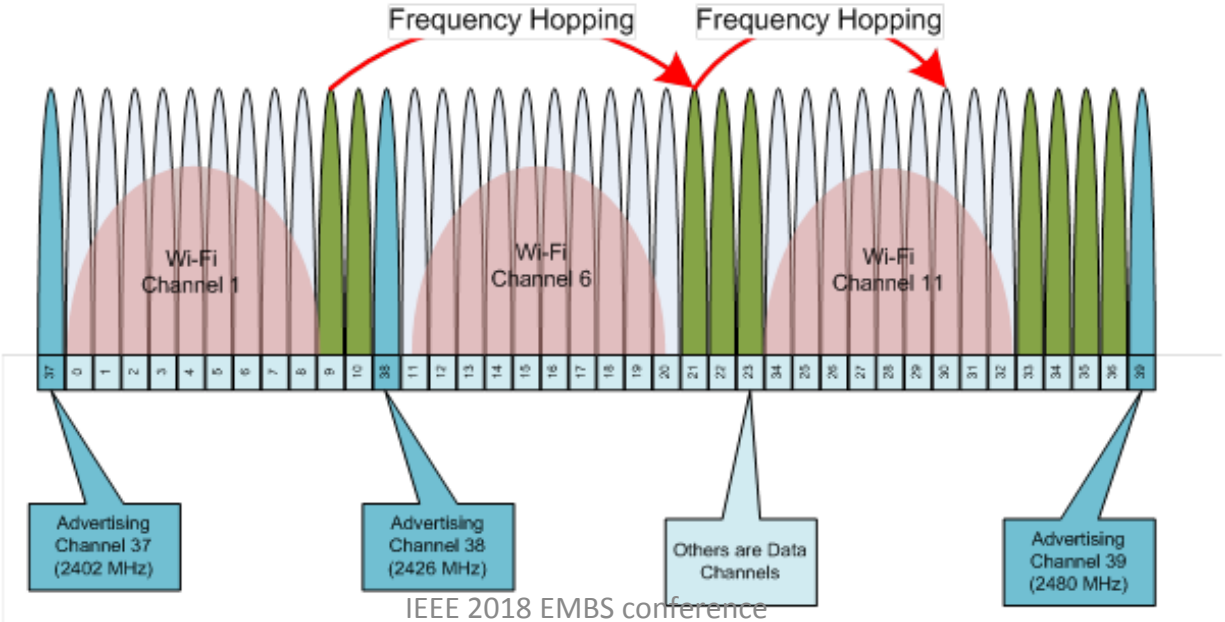
- Bluetooth® wireless technology introduction
- Bluetooth benefits for medical systems
- The Medical Internet of Things
- Bluetooth coexistence
- Bluetooth security
- Bluetooth medical device regulatory

Bluetooth wireless technology introduction

- Provides connectivity for all mobile platforms
  - Ubiquitous
  - Low power
  - Low cost
  - Audio & Data transports
  - Good range – typically 50 feet connection to iPhone/Android
- Operates well (cooperates) in RF noisy/crowded environments
  - Fast 2.4 GHz FHSS radio (Frequency Hopping Spread Spectrum)
  - Adaptive Frequency Hopping
  - Error detection, retransmission, error correction
- Bluetooth 4.0 added Bluetooth low energy transport
  - Greatly improved cost/power (CFR2032 coin cell operation)
  - Lower data rates, (100's of Kbps → 1 Mbps)
  - Greatly simplified communications stack
  - Flexibility for custom services & profiles
  - Beacons
  - Mesh

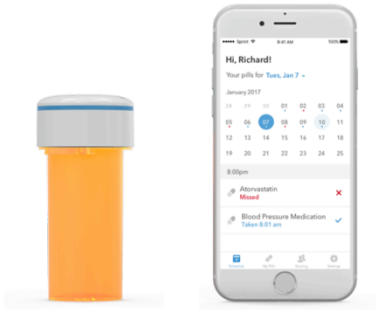
The Bluetooth low energy technology basics

- 2.4 (– 2.485) GHz, Frequency Hopping Spread Spectrum technology
- 40 discrete channels, 2 MHz wide, psuedo-random hopping sequence (1600 hops/second)
- Dedicated Advertising channels
- Adaptive frequency hopping (AFH) for coexistence/interference
- 10dBM maximum power output; increased for BT5
- ~50 meters depending on platform/implementation
- ~100 Kbps realizable throughput depending on platform/implementation



Bluetooth benefits for medical systems

- Ubiquitous support – it is everywhere
- Excellent coexistence with WiFi
- Low cost, low power operation enables mobile and wearable devices and systems
- First hop to the cloud
- Personal Area Network
- Medical Internet of Things

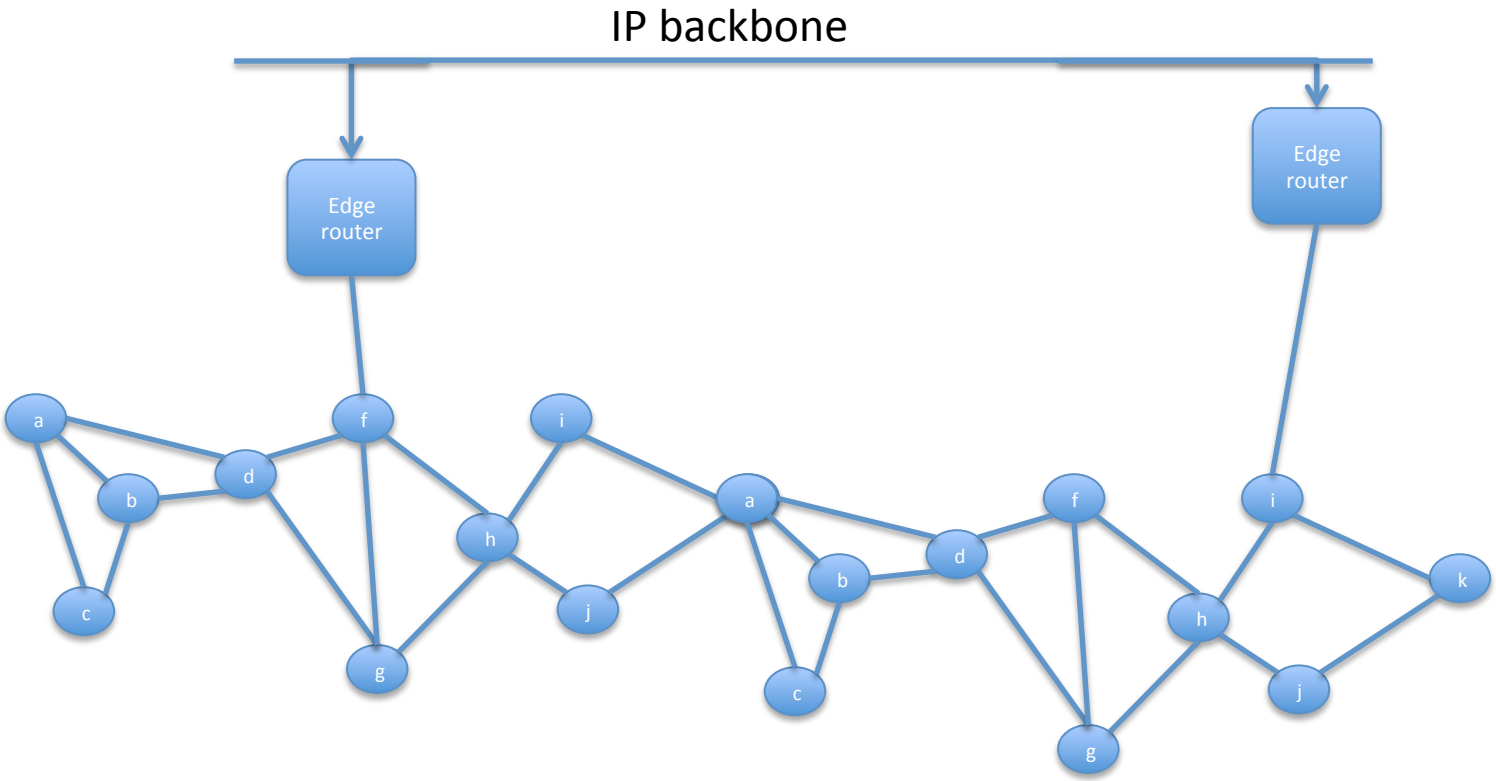


Beacons

- Bluetooth low energy Generic Access Profile (GAP) specifies advertiser/scanner to establish connections
- An advertisement can put out any information and doesn't require connection
- A beacon is a structured advertisement
  - Undirected broadcast of data
  - Think UDP as contrasted with TCP
- Two ad-hoc standards have evolved
  - iBeacon - iOS
  - Eddystone − Google/Android

Bluetooth mesh 1.0

- Version 1.0 uses advertising and repeaters
- “Flood” network
- Doesn’t require Bluetooth 5

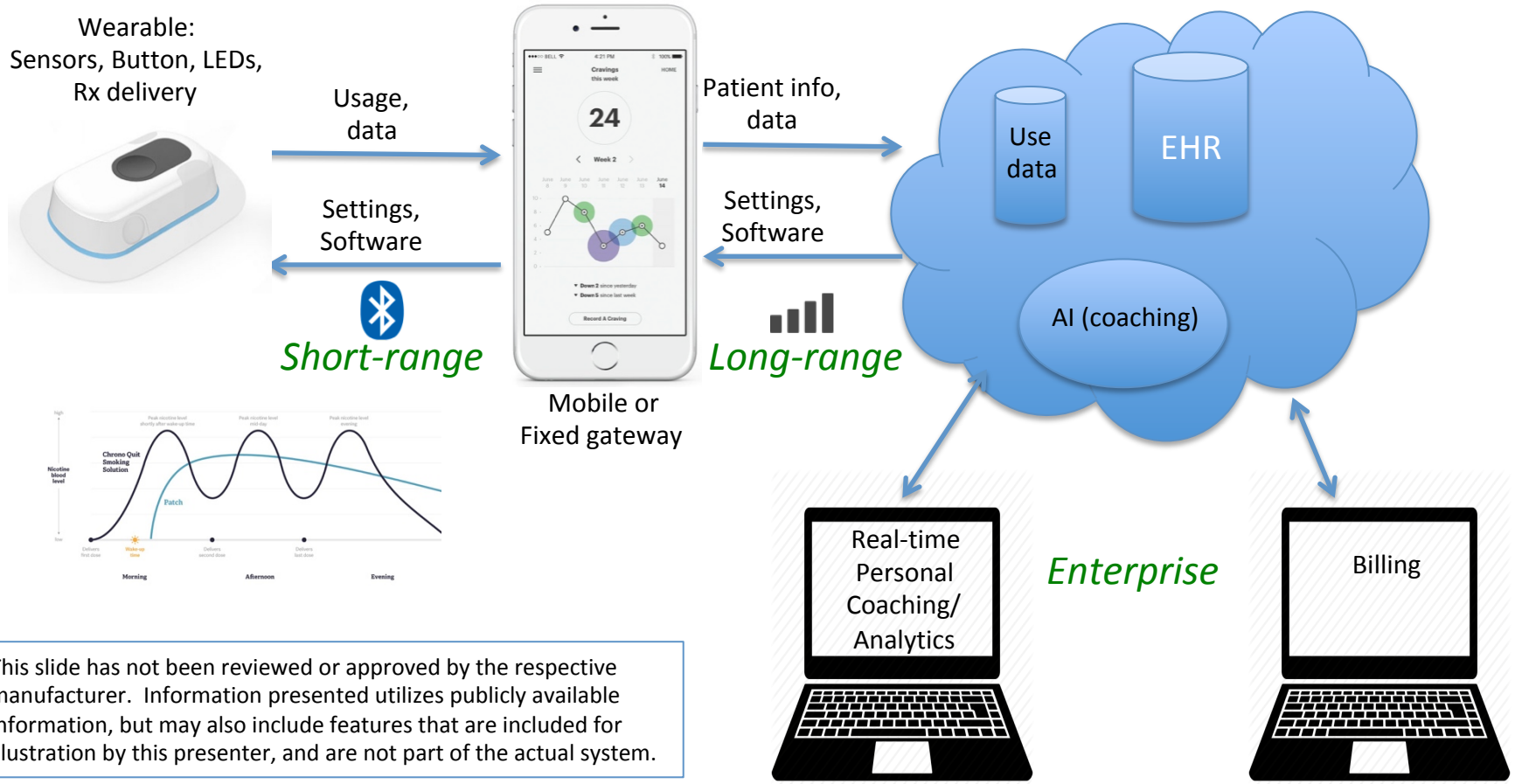


Bluetooth 5

- Released at the end of 2016
- Long range
  - Up to 4x (~200 meters)
  - Tradeoff: lower speed
  - Also higher reliability…
- High speed
  - Same power
  - Tradeoff: reduced range
- Increased advertising capability
  - More broadcast data
  - Advertising on data channels to reduce congestion
  - Chaining
  - Periodic advertising
- Additional coexistence measures
- All of the above are optional and are negotiated after connection for backwards compatibility

The Medical Internet of Things Architecture

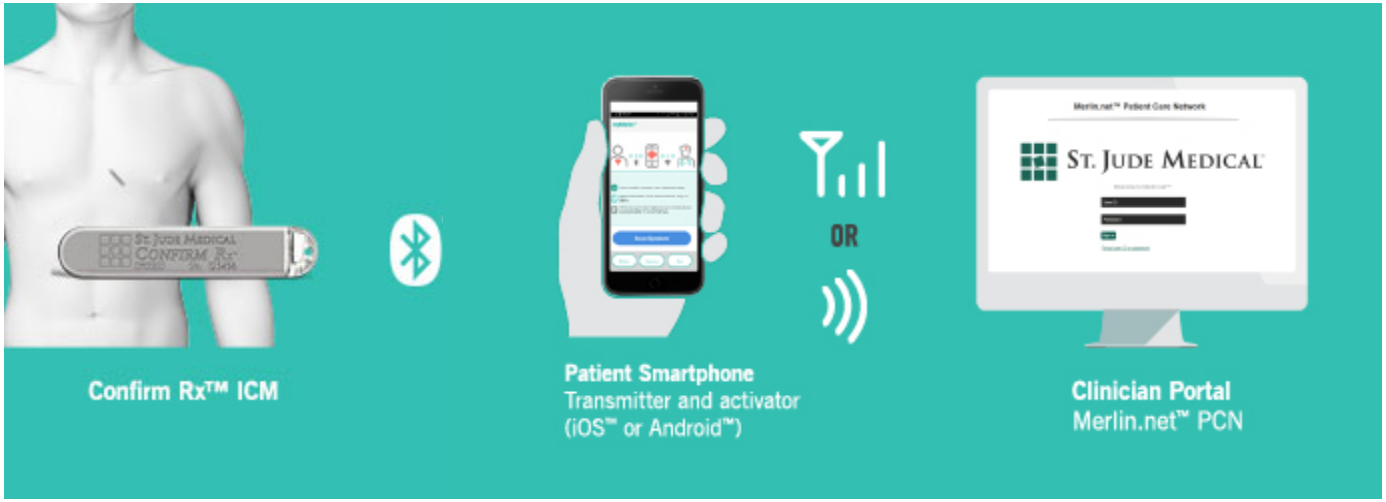
Adapted from Chrono Therapeutics smoking cessation solution (investigational)



This slide has not been reviewed or approved by the respective manufacturer. Information presented utilizes publicly available information, but may also include features that are included for illustration by this presenter, and are not part of the actual system.

Insertable Cardiac Monitor

- Abbott Confirm™ RX ICM
- “The world’s first smartphone-compatible ICM”
- FDA cleared October, 2017



This slide has not been reviewed or approved by the respective manufacturer. Information presented utilizes publicly available information, but may also include features that are included for illustration by this presenter, and are not part of the actual system.

Bluetooth coexistence mechanisms

- Frequency Hopping Spread Spectrum (FHSS)
- Adaptive Frequency Hopping (AFH)
- Error handling
  - Detection
  - Packet retransmission
  - Forward Error Correction

Bluetooth-specific cybersecurity

- Security/authentication without physical connection
  - Spoof/mimic data connections
  - Eavesdropping
- Man in The Middle (MTM) attacks (especially during pairing)
- Over The Air (OTA) upgrades
- Setting changes
- Advertising promiscuously

Bluetooth security features

- FHSS inherently designed to minimize eavesdropping (but that was for WWII)
- Pairing and bonding modes depending on requirements and user interface
  - Note that old-style PIN has been deprecated and should not be used in new devices
- Caution: “Just works” mode is available with no encryption or authentication
- 128-bit AES for encryption, several methods/means for authentication
- Mode and level definition allows for appropriate implementations
  - Security Mode 1 Level 4: strongest including authenticated low energy Secure Connections pairing & Elliptic Curve Diffie-Hellman (ECDH) based encryption
  - Security Mode 1 Level 3 requires authenticated pairing & encryption but does not use ECDH-based cryptography and provides limited eavesdropping protection due to weak encryption
  - Other security modes/levels allow unauthenticated pairing (meaning no MITM protection is provided during cryptographic key establishment)
  - Some modes/levels do not require any security at all
- *It is essential to perform appropriate cybersecurity and risk analysis and implement and test appropriately*

Cybersecurity recommendations

- Use Bluetooth 4.2 and later
- Security by design, not obfuscation
  - End-to-end solution, both connectivity and at rest
  - Design for Cybersecurity
  - Design for Privacy
- Limit information: don’t exchange unnecessary data
- Limit vulnerabilities
  - Limit time and accessibility
    - Pairing
    - Security key exchanges
  - Don’t use unnecessary profiles
  - Set and enforce policies
- Don’t advertise promiscuously

The 3 groups of regulators

- Medical regulatory *requirements*
  - US FDA
  - EU Medical Device Regulation (and what about the UK?)
  - Other countries/regions per marketing
- Wireless standards bodies
  - Bluetooth SIG – legal *requirement*
  - No IEEE formal approval (IEEE 802.15.1)
- Radio regulators - *required*
  - FCC – US
    - SAR for patient-worn devices)
  - IC – Canada
  - EU – ETSI, R&TTE
  - Japan – MIC
  - Other countries/regions per marketing

… and the 4th group: “interoperability”

- Interoperability is a dual-edge sword
  - Market dominance
  - Regulatory scope
- AAMI − primarily for in-hospital devices
- Bluetooth SIG profiles
  - Bluetooth Transcoding Whitepaper
  - Health/medical profiles − use them if you wish
  - With Bluetooth low energy you can make your own
- Continua Alliance?
- FHIR, HL7, … if utilized

Regulatory considerations

- Safety and efficacy for the intended use in the intended environment(s)
- Interference & Coexistence
  - Ad-hoc testing based on environment for Intended Use
  - RF Guidance documents and industry standards
- Latency & Throughput
  - Consider degradation again based on environment
- Cybersecurity
- NIST
- References at the end of this presentation

Summary

- Bluetooth wireless technology provides an excellent communications method for medical devices and systems
- As with all wireless technologies specification, design, implementation, and testing are key elements

Contact information

Bill Saltzstein

Code Blue Consulting

www.consultcodeblue.com

billsalt@consultcodeblue.com

425-442-5854

Selected Cybersecurity References

- Healthcare Industry Cybersecurity Task Force report
  - https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
- 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
- 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
- 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

Additional FDA guidance

- FDA landing page for Digital Health
  - http://www.fda.gov/medicaldevices/digitalhealth/
- General Wellness: Policy for Low Risk Devices
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/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
- Software as a Medical Device (SAMD): Clinical Evaluation
  - https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM524904.pdf
- Clinical and Patient Decision Support Software (draft)
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm587819.pdf
- Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act (draft)
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm587820.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
- Enforcement discretion
  - http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm
- Deciding When to Submit a 510(k) for a Software Change to an Existing Device
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm514737.pdf
- Design Considerations and Pre- market Submission Recommendations for Interoperable Medical Devices
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482649.pdf

AAMI

- TIR57: Principles for medical device security—Risk management
  - https://standards.aami.org/kws/public/projects/project/details?project_id=876
- TIR69: Risk Assessment of radio-frequency wireless coexistence for medical devices and systems
  - https://standards.aami.org/kws/public/projects/project/details?project_id=1114
- ANSI C63.27-2017: American National Standard for Evaluation of Wireless Coexistence
  - https://standards.ieee.org/findstds/standard/C63.27-2017.html

Bluetooth SIG

- Transcoding (and other) Whitepapers:
  - https://www.bluetooth.com/develop-with-bluetooth/white-papers
- Bluetooth 5 Standard:
  - https://www.bluetooth.com/specifications/bluetooth-core-specification

Acronyms (google for definitions/information)

- AFH − Adaptive Frequency Hopping
- BLE − Bluetooth low energy
- BR/EDR − Basic Rate or Enhanced Data Rate (See Bluetooth specifications)
- FHSS − Frequency Hopping Spread Spectrum radio transport
- ISM − Industrial, Scientific, and Medical: frequency bands allocated by the FCC
- LAN − Local Area Network: IEEE 802.3
- MBAN − Medical Body Area Network
- MDDS − Medical Device Data System (see Reference section)
- NFC − Near Field Communications
- PHI − Protected Health Information
- SIG − Special Interest Group, in this case the Bluetooth SIG
- WiFi − Wireless Fidelity: IEEE 802.11 specifications
- ZigBee − Wireless standard from the ZigBee Alliance, based on IEEE 802.15.4