ORTHOGONAL™ & MedSec

Meeting FDA Requirements for BLE Mobile Medical Apps

September 20th, 2023 | 12 PM EDT

Bernhard Kappe
CEO & Founder
Orthogonal

Buddy Smith
Director of Technical Consulting
MedSec

Randy Horton
Chief Solutions Officer
Orthogonal

The Bluetooth Series – from Orthogonal and MedSec

The Bluetooth Series from Orthogonal and Medsec - Spring/Summer/Fall of 2023

- Webinars, Blogs, Whitepapers, etc.
- To learn more:
  - Monthly email notifications
  - https://orthogonal.io/insights/bluetooth/
  - https://orthogonal.io/bluetooth-low-energy-webinar-series/

What challenges are you facing? -> What content do you want us to cover?

Bluetooth + Consumer Mobile Devices (e.g., smartphones) power many modern connected medical device systems

- Unfortunately, it doesn't "just work"
- Fortunately, it doesn't have to be as a hard as it often currently is

FDA Basics

U.S. Department of Health and Human Services
Food and Drug Administration
FDA

The FDA's mandate is to foster safety *and* innovation.

Types of FDA Submissions:

- PMA - high risk devices, changes require approval, more scrutiny.
- De Novo - New device category and *sets a precedent* for 510(k)s.
- 510(k) - substantial equivalence.

FDA Basics (Continued)

- Design controls: Appropriately control your risk and ensure effectiveness.
- The riskier the device is, the more you need to do to reduce risk to acceptable levels and demonstrate effectiveness of your risk controls.
- New or pushing the envelope? The FDA will be cautious. (Remember, precedent!)
- The FDA sees a lot of devices, adverse event reporting, and recalls.
- If they don’t see problems, they reduce the burden. If they see issues, they issue guidance.
- Not all reviewers are created equal.

How This Applies to Bluetooth and BYOD

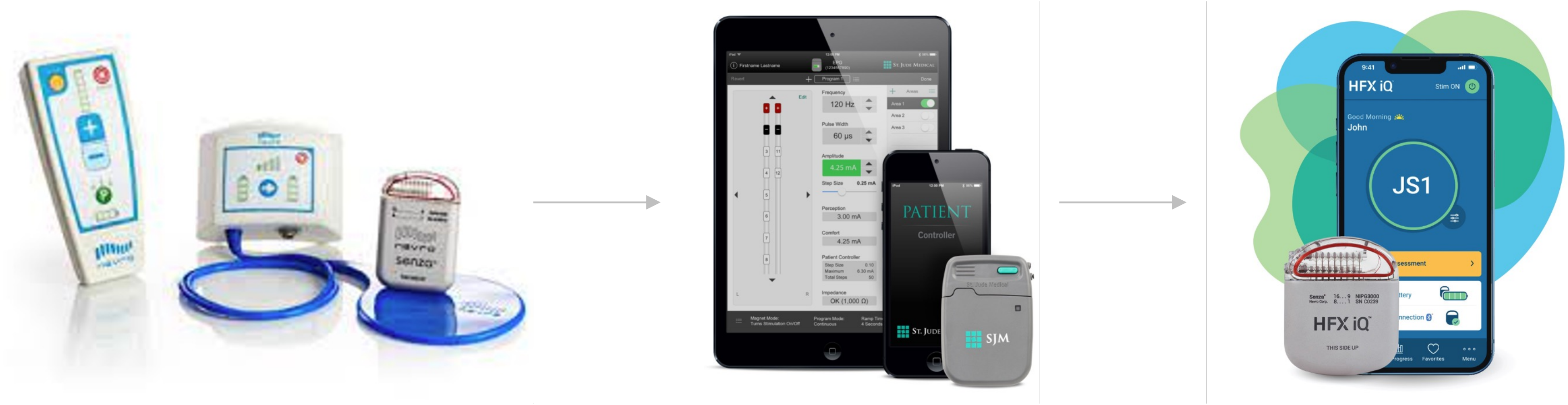
Lower Risk & Complexity

- Single Measure (e.g. Pulse Ox)
- Unidirectional Communication
- MDM
- 510(k)

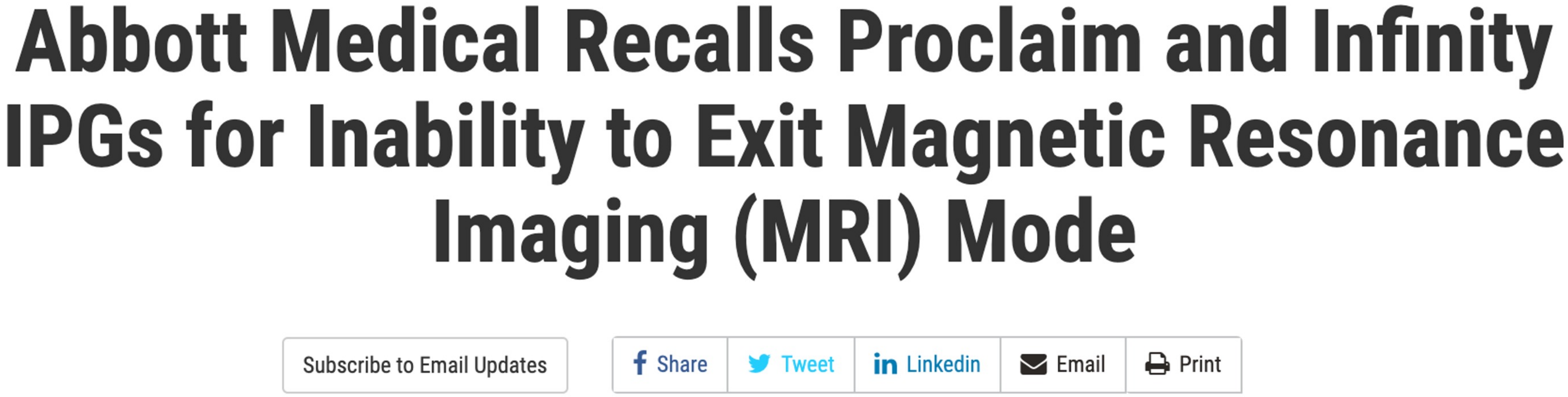
Higher Risk & Complexity

- High Risk Devices (e.g infusion pump)
- Continuous Real Time (CGM)
- Device Control
- AI Algorithm to Change Therapy
- Patient Facing
- BYOD
- Unavailability Causes Harm
- Interoperable
- SDK

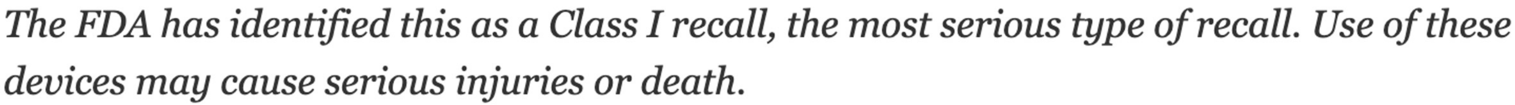
Example: Spinal Cord Nerve Stimulators



July 18, 2023

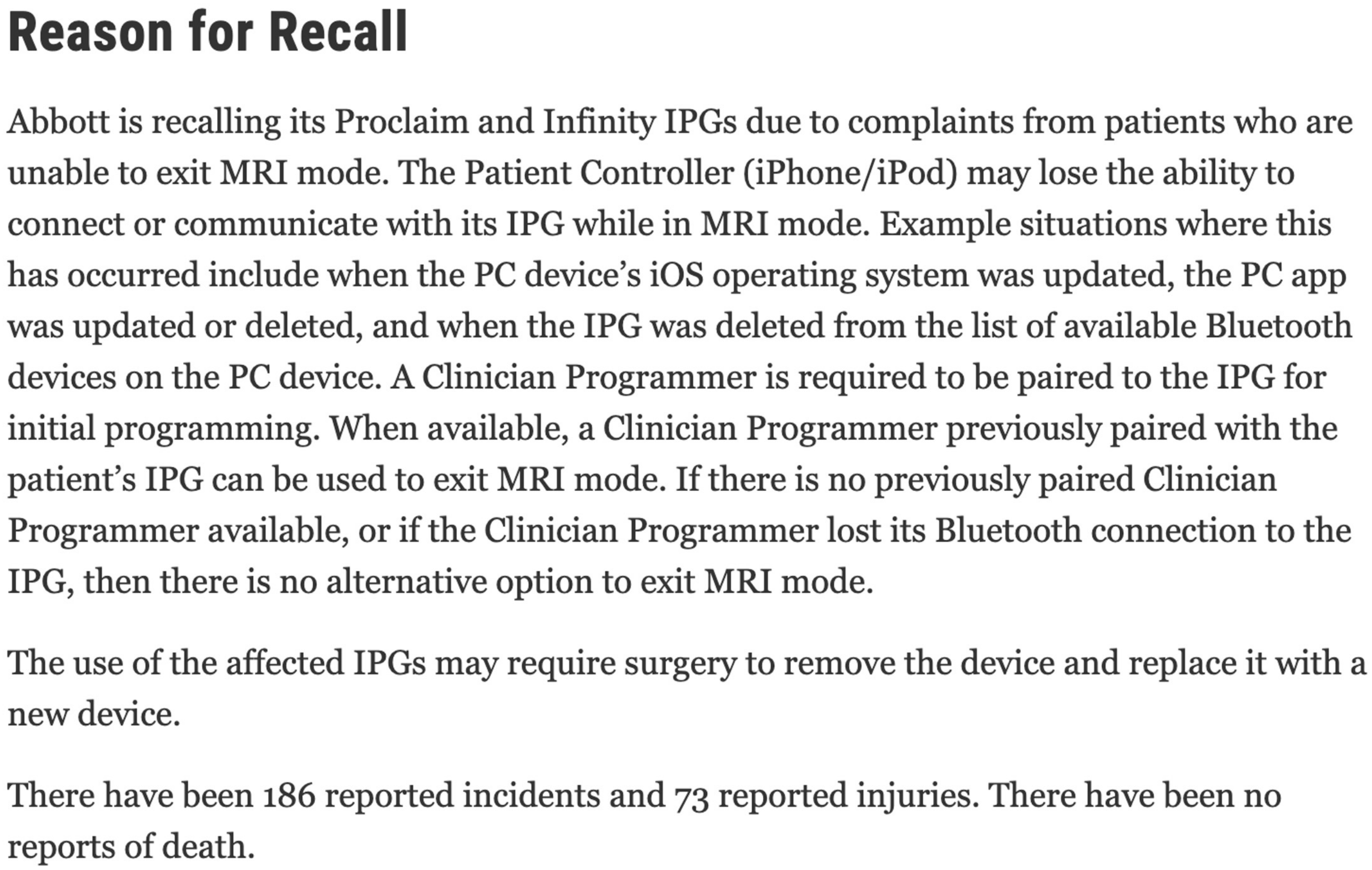


Abbott Medical Recalls Proclaim and Infinity IPGs for Inability to Exit Magnetic Resonance Imaging (MRI) Mode



The FDA has identified this as a Class I recall, the most serious type of recall. Use of these devices may cause serious injuries or death.

https://www.fda.gov/medical-devices/medical-device-recalls/abbott-medical-recalls-proclaim-and-infinity-ipgs-inability-exit-magnetic-resonance-imaging-mri-mode



Reason for Recall

Abbott is recalling its Proclaim and Infinity IPGs due to complaints from patients who are unable to exit MRI mode. The Patient Controller (iPhone/iPod) may lose the ability to connect or communicate with its IPG while in MRI mode. Example situations where this has occurred include when the PC device's iOS operating system was updated, the PC app was updated or deleted, and when the IPG was deleted from the list of available Bluetooth devices on the PC device. A Clinician Programmer is required to be paired to the IPG for initial programming. When available, a Clinician Programmer previously paired with the patient's IPG can be used to exit MRI mode. If there is no previously paired Clinician Programmer available, or if the Clinician Programmer lost its Bluetooth connection to the IPG, then there is no alternative option to exit MRI mode.

The use of the affected IPGs may require surgery to remove the device and replace it with a new device.

There have been 186 reported incidents and 73 reported injuries. There have been no reports of death.

BYOD for High Risk Devices?

- Trend for more complex, more functions on the smartphone over time. For high risk devices, have some pullback to MDR and dedicated devices.
- Too risky, too hard to maintain. Looking at BYOD differently, looking to reduce the attack surface. Go back to MDM?

Questions to Consider

- Usability if the phone is not locked down.
- Critical alerts, DND, mute button. Can the average consumer figure this out? 60 to 70 year olds?
- What sensors on the phone do you really need? Camera? Upload photos of what they ate to a patient diary?
- Can you detect if it is an issue?
- Can you detect what else is running?
- What do you fix quick, what is slower. (Cybersecurity guidance helps here.)

Cybersecurity

- Big point of emphasis for FDA.
- Multiple revisions of pre and post market guidance.
- Multiple Function Device Guidance is a workhorse for the FDA.
  - Boundaries for patient risk and non-device functions.
  - But not for cybersecurity – need to take the whole system, external interfaces and dependencies.

We don’t trust this, right?

Cybersecurity for Bluetooth

Don’t assume Bluetooth is secure.

- Have security controls under the Bluetooth layer. (Encryption at rest, in transit. Out of bound pairing. Data and communication over the interface, etc.)
- Detect jailbroken phones. Decide, based on risk, how the use needs to change. Deny access? Just notify? Limit functionality?
- How do you control for third party apps? Do they use the same services? Are they updated? What are the security holes? (e.g. Chrome browser on the smartphone.)
- SDK Integration with other apps – who is responsible for security? Unidirectional? Bidirectional? Can be a high bar – need to work out shared security certificates and legal aspects for SDK interoperability. Trusted communication.

Scoping, Analysis and Testing

- Operate in the worst case scenario
  - Most outdated phone and OS you support.
  - Claim 10 feet, test at 20 feet.
- Hardware and environment
  - Device in body, smartphone in a case in the back pocket. Saline solution, mannequins.
  - Create RF interference (baby monitor, microwave, etc.)
  - Code to see where it falls apart, collect data for operational diagnostics.
- Chipsets and Bluetooth – same chip manufacturer, more confidence.
- Scope your threat modeling more broadly.
- Pen Testing at a system level.

Scoping, Analysis and Testing

- Initially, you may be asked to do something that others later won’t be asked to do.
  - Example: Human Factors Testing – can people download the app?
- Over time, you learn what is of value and where things actually break, based on actual observation. So does the FDA.
- Once you have agreed to a regimen for monitoring and testing, it is hard to change. But if you come with evidence, and it correlates to what the FDA is seeing in the market, it can be worth negotiating a change.

Patient Satisfaction

- For many connected device companies, the biggest challenge has been not FDA satisfaction but customer satisfaction.
    - High reliability means high satisfaction. Customer satisfaction is more difficult.
- The expectation from patients is that it just works.
- Problems can be hard to reproduce.
- Main customer gripe for continuous background monitoring (like CGMs) – things that kill the app or force you to restart.
- OS not under your control. Apple does housekeeping – kill the background processing.
- You have messages to restart – but at night, when you're sleeping…
- Need to look at and gracefully handle edge cases.

Orthogonal Edge Case Library

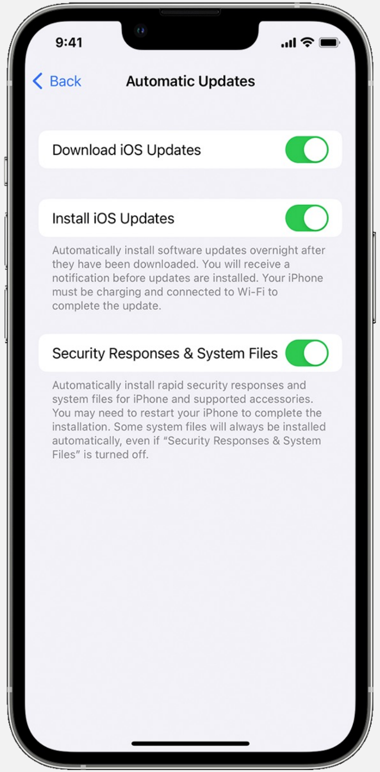
ORTHOGONAL™

Bluetooth
Edge Case
Library

August 2023

- Accumulated over 12 years and dozens of BLE medical device systems.
- Detailed issue description, scenarios, differences between operating systems and actions.
- Includes acceptance criteria and testing methods.
- Reviewed as part of any new product development effort with BLE.
- New edge cases added as we discover them.

Comorbidities and Multiple Device Apps



9:41

< Back — Automatic Updates

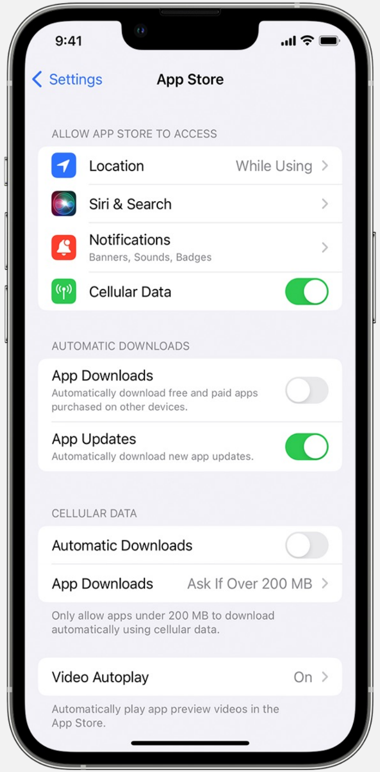
Download iOS Updates ☑

Install iOS Updates ☑

Automatically install software updates overnight after they have been downloaded. You will receive a notification before updates are installed. Your iPhone must be charging and connected to Wi-Fi to complete the update.

Security Responses & System Files ☑

Automatically install rapid security responses and system files for iPhone and supported accessories. You may need to restart your iPhone to complete the installation. Some system files will always be installed automatically, even if "Security Responses & System Files" is turned off.



9:41

< Settings — App Store

ALLOW APP STORE TO ACCESS

Location — While Using >

Siri & Search >

Notifications >
Banners, Sounds, Badges

Cellular Data ☑

AUTOMATIC DOWNLOADS

App Downloads □
Automatically download free and paid apps purchased on other devices.

App Updates ☑
Automatically download new app updates.

CELLULAR DATA

Automatic Downloads □

App Downloads — Ask If Over 200 MB >

Only allow apps under 200 MB to download automatically using cellular data.

Video Autoplay — On >

Automatically play app preview videos in the App Store.

- Many patients have comorbidities.
- Many have devices and apps for those different diseases.
- Some are instructed to leave auto-updates off, others to leave auto updates on.
- This happens even if the devices and apps are from the same company!

Don’t Forget About Other Regulations

- DOD
- VA
- OMB
- FCC
- FAA
- OSHA (if used by clinicians and techs)

Biggest Mistakes

Mistake	**Best Practice**
Everything, Everywhere, All at Once	Incremental Strategy
Pen Test App and Device Separately	Test as a System
Bluetooth is Secure Enough	Secure By Design, Secure Other Layers
Just Test The Latest, Best Case	Test the Worst Case
No Edge Case Mitigations and Testing	Risk of Edge Cases
Too Much Testing, Not Enough Analysis	Scope, Analyze, Mitigate, Validate