# General Security Lifecycle for Medical Devices

- Procurement
  - Manufacturer
  - Reseller
- Configuration
  - Systems
  - Network
  - Interfaces
- Maintenance and Updates
- End of Life

# How this is starting to look for SMART-types

- Heavy emphasis on procurement
- Upfront Risk Assessment – not just security but failures in general
  - Clinician Driven – comparable to research-driven governance
  - Can you adjust/update/patch?
  - Is there a sensible recall pathway?
  - Upstream and downstream dependencies
- Testing – covers every technical skillset and more
  - Network
  - Application
  - Hardware
  - Encryption
  - Reverse engineering

# Hopeful signs

- IoT frameworks
- Secure low level programming paradigms (e.g. Rust, Swift)
- Lightweight security agents
- Sandboxing and micro-virtualization
- Changes in enterprise network security -- the closer security controls are to the device the better

# Application whitelisting – code registers

- Does not solve every problem, such as authentication
- Most effective control for malware distribution
- Emphasizes the need for port/process controls prior to shipping
- 80 percent solution – but an important 80 percent