Patching process

- Device OS and architecture variability
- Future plan: Higher patch frequency
- Future plan: Standardized notification channel
- Global regulatory mapping
- Notification to HDO: Call
- Notification to HDO: Email
- Notification to HDO: Letter
- Notification to HDO: Proprietary portal
- Notification to HDO: Regular service meetings
- Notification to HDO: Security Advisory
- Notification to HDO: Security white paper
- Patch delivery: Field Safety Notification
- Patch delivery: Remote
- Patch delivery: Service technician
- Patch frequency: Field Safety Notification patch
- Patch frequency: Regular update releases
- Update bundling: Considerations
- Update bundling: Prevalence
- Validation testing

Risk management

- Mitigation: Device-level security measures
- Mitigation: Mandated Use: Device Configuration
- Mitigation: Mandated Use: Network security
- Mitigation: Mandated Use: Physical security
- Mitigation: Security Patch
- Process: Internal risk level determination
- Risk approach: FDA
- Risk criteria: Device context of use
- Risk criteria: Device network connections
- Risk criteria: Exploitability
- Risk criteria: Patient Safety
- Tool: Central security requirements framework
- Tool: SBOM
- Unrealistic risk scenarios

Customer (HDO) observations

- Country differences
- Expectations: Distrust device's security implementations
- Expectations: Faster patch releases
- Expectations: Higher patch frequency
- Expectations: Stricter security and privacy requirements
- Expectations: Variations among HDO departments
- Practice: Compensating network security measures
- Practice: High prevalence of legacy device use
- Practice: No full patch install coverage
- Update delivery considerations: Avoid functional changes
- Update delivery considerations: Control update process
- Update delivery considerations: Costs of updates
- Update delivery considerations: Distrust towards manufacturer
- Update delivery considerations: Ensure continued medical use
- Update delivery preferences: Install by service technicians
- Update delivery preferences: Low demand for remote install

Challenges

- Customers' distrust
- Customers' lack of awareness
- Dispatching technicians: Coordination Costs
- Evolving threat landscape
- Increasing vulnerabilities
- Internal negotiations for security
- Regulatory pressure: Continuous validation with faster releases
- Regulatory pressure: Costly validation testing
- Regulatory pressure: Design lock-in
- Remote update capability implementation
- Short time frame for emergency patch rollout

Codebook for the interviews with product security specialists at medical device manufacturers.