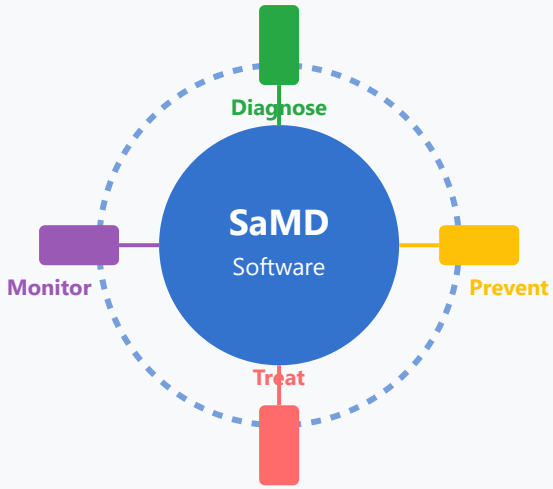
Software as Medical Device

- SaMD framework
- Risk categorization
- Quality management
- Cybersecurity
- Updates and modifications

1. SaMD Framework

Definition & Scope



Software as a Medical Device (SaMD) is software intended to be used for medical purposes that performs these functions without being part of a hardware medical device. The framework establishes a consistent approach for classification and regulation across different jurisdictions.

- **Medical Purpose:** Software must have intended medical use (diagnosis, prevention, monitoring, treatment)
- **Standalone Operation:** Functions independently without being integrated into hardware
- **Clinical Decision Support:** Provides information for healthcare decisions
- **International Standards:** Based on IMDRF guidelines for global harmonization

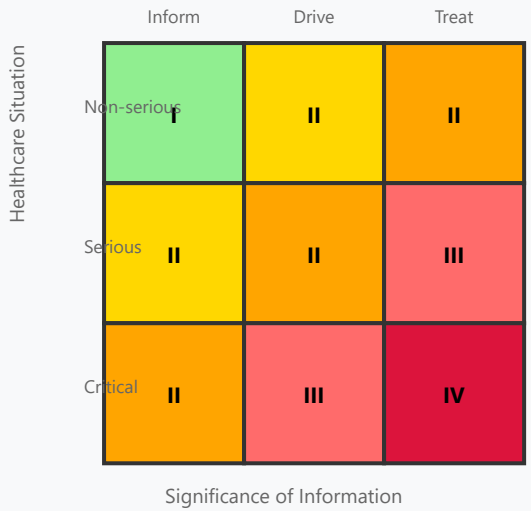
Examples

• AI algorithms for radiology image analysis
• Mobile apps for diabetes management
• Clinical decision support systems
• Remote patient monitoring software

2. Risk Categorization

Risk Classification Matrix

SaMD is categorized based on two dimensions: the significance of the information provided and the healthcare situation or



condition. This creates a risk-based classification from Class I (lowest risk) to Class IV (highest risk).

- **Class I:** Lowest risk - informing clinical management for non-serious conditions
- **Class II:** Low-moderate risk - driving or informing for serious conditions
- **Class III:** Moderate-high risk - driving clinical management for critical situations
- **Class IV:** Highest risk - treating or diagnosing critical, life-threatening conditions

Impact on Regulation

Higher risk classes require more rigorous regulatory oversight, clinical validation, and post-market surveillance. The classification determines premarket approval requirements and ongoing compliance obligations.

3. Quality Management System

ISO 13485 & ISO 14971

Quality management systems for SaMD must comply with ISO 13485 (Quality Management for Medical Devices) and ISO 14971 (Risk Management). These standards ensure systematic processes for design, development, production, and post-market activities.

- **Design Controls:** Systematic approach to software development with verification and validation
- **Risk Management:** Continuous identification, analysis, and mitigation of risks throughout lifecycle
- **Document Control:** Comprehensive documentation of all processes, changes, and decisions
- **CAPA System:** Corrective and Preventive Action processes for continuous improvement
- **Post-Market Surveillance:** Ongoing monitoring of device performance and safety

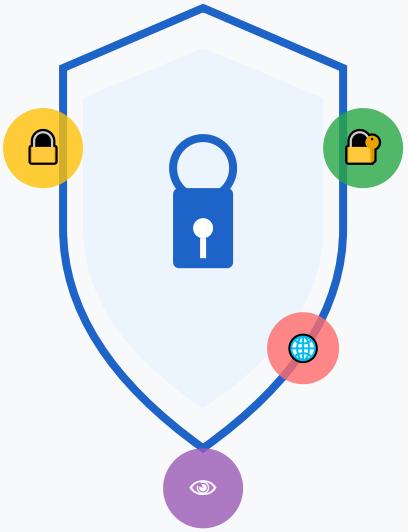
Key Deliverables

• Software Requirements Specification
• Design Documentation
• Risk Management File
• Verification & Validation Reports
• Technical Documentation

4. Cybersecurity Requirements

FDA & International Guidelines

Cybersecurity is critical for SaMD as these devices often handle sensitive patient data and can impact patient safety. Manufacturers must implement comprehensive cybersecurity controls throughout the product lifecycle, following FDA premarket and postmarket guidance.



- **Threat Modeling:** Systematic identification of potential cybersecurity vulnerabilities and attack vectors
- **Secure by Design:** Building security into architecture from the beginning, not as an afterthought
- **Data Protection:** Encryption of data at rest and in transit, access controls, and authentication
- **Network Security:** Secure communication protocols, firewalls, and network segmentation
- **Vulnerability Management:** Regular security assessments, penetration testing, and patching
- **Incident Response:** Documented procedures for detecting and responding to security events

Regulatory Submissions

Premarket submissions must include a Software Bill of Materials (SBOM), security risk assessment, and evidence of security controls implementation.

5. Software Updates & Modifications

Change Management Process

Software modifications require careful evaluation to determine if they constitute a significant change requiring new regulatory submissions. Changes must be managed through a documented change control process with appropriate testing and validation.

- **Minor Updates:** Bug fixes, security patches, performance improvements - may not require new submission
- **Major Updates:** New features, changed intended use, modified algorithms - typically require regulatory review
- **Change Assessment:** Evaluate impact on safety, effectiveness, and intended use
- **Version Control:** Maintain comprehensive documentation of all software versions and changes
- **Validation Requirements:** Each change must be validated to ensure it doesn't introduce new risks
- **User Notification:** Clear communication to users about updates and their significance

FDA Guidance Considerations

FDA's Digital Health Innovation Action Plan and Pre-Cert Program aim to streamline updates for established manufacturers while maintaining patient safety. AI/ML-based SaMD may use predetermined change control plans for continuous learning.

SaMD Regulatory Strategy

Pre-Market Activities

- Define intended use and indications

Post-Market Activities

- Monitor device performance
- Track adverse events

- Conduct risk classification
- Establish quality management system
- Perform clinical evaluation
- Develop cybersecurity documentation
- Prepare regulatory submission

- Manage software updates
- Address cybersecurity vulnerabilities
- Conduct periodic safety reviews
- Maintain regulatory compliance

Key Success Factors

- Early regulatory engagement
- Robust clinical evidence
- Comprehensive documentation
- Cross-functional collaboration
- Continuous monitoring
- Proactive risk management

Common Challenges

- Evolving regulatory landscape
- AI/ML validation complexity
- Cybersecurity threat evolution
- International harmonization
- Rapid technology advancement
- Clinical evidence generation

Conclusion

Successful SaMD development requires a comprehensive understanding of regulatory requirements, a robust quality system, proactive risk and cybersecurity management, and continuous adaptation to evolving standards. Early planning and regulatory

engagement are critical for market success.