SAFETY OS™

CONFIDENTIAL

Software as a Medical Device (SaMD) | Technical Specification

Version:3.1(US Market)
Date: November 2025

Class II SaMD (FDA 510k Pending)

1. SYSTEM ARCHITECTURE (THE 4-LAYER STACK)

Proprietary architecture decouples clinical intent from robotic actuation, ensuring safety regardless of hardware.

Layer 1: Hardware Abstraction Layer (HAL)

- Universal translator API for OEM-agnostic clinical commands
- Compatibility: Unitree (G1/R1), Tesla (Optimus Gen 3), Boston Dynamics (Atlas)
- Protocol: gRPC / ROS 2 Bridge

Layer 2: The Safety Kernel (Real-Time Control)

- Immutable safety boundaries - cannot be overridden by AI
- Standards: ISO 13485 Certified, IEC 62304 Class C Safety Critical
- Latency: <10ms hard real-time response for collision avoidance
- Force Limiting: Dynamic torque capping based on patient frailty score

Layer 3: Clinical Logic Engine

- Manages Activities of Daily Living (ADLs) and Care Plans
- Modules: Fall Detection, Medication Adherence, Ambulation Support, Hydration
- AI Model: Hybrid Neuro-Symbolic (LLM conversation + Deterministic action)

Layer 4: Cloud & Compliance

- **Deployment:** Architecture designed for native hosting within EHR environments (Epic App Orchard / Oracle Health)
- **Governance:** Architecture aligned with TOGAF ADM principles for Enterprise IT integration
- **Logging:** “Black Box” immutable audit trail linked directly to Patient ID

2. INTEROPERABILITY & DATA

EHR Integration

- **Standard: SMART** on **FHIR** native application framework
- **Data Transport:** Bi-directional HL7 FHIR R4 (Service Request & Observation resources)
- **Identity:** Single sign-on (SSO) via Hospital Active Directory (OAuth 2.0)

Security

- **Data at Rest:** AES-256 Encryption
- **Data in Transit:** TLS 1.3
- **Architecture:** Zero Trust Network Access (ZTNA)

HL7 FHIR

CERTIFIED ISO 13485

3. DEPLOYMENT REQUIREMENTS

- **Connectivity:** 5G / Wi-Fi 6E (Required for Telepresence fallback)
- **Edge Compute:** Minimum NVIDIA Orin (or equivalent) on-robot for local inference
- **Offline Mode:** Core Safety Kernel operates 100% locally without internet connectivity

4. REGULATORY PATHWAY

- **US FDA:** 510(k) Submission (Class II SaMD) **Predicate:** Remote Patient Monitoring Systems
- **AI AGility: PCCP** (Predetermined Change Control Plan) included for post-market algorithm updates
- **Cybersecurity:** Compliant with FDA 'Cybersecurity in Medical Devices' Guidance (2023)

PatientCentric Care.AI

TOGAF® Enterprise Architecture Leader THE Open GROUP