

Medical CE & FDA Technical Compliance Register: Post-Market Surveillance Data Archiving Protocol

CLINICAL SAFETY POSITIONING

The Post-Market Surveillance Data Archiving Protocol (PMS-DAP) constitutes a critical, non-clinical software and process infrastructure layer within the medical aesthetic device ecosystem. Its primary function is to ensure continuous, auditable, and secure collection of device performance data, adverse event reports, and clinical outcome metrics following market release. This protocol is engineered to satisfy the rigorous post-market obligations mandated by the Medical Device Regulation (EU) MDR 2017/745, FDA 21 CFR Part 803 (Medical Device Reporting), and ISO 13485:2016 clause 8.2. This document serves as the official technical compliance register and operational datasheet for the PMS-DAP as deployed across the OEM aesthetic device fleet. It defines the digital architecture, data integrity safeguards, and retrieval workflows that enable clinics to transition from reactive incident logging to proactive, evidence-based safety surveillance. The protocol is not a standalone physical device but a validated firmware and cloud-synchronized module integrated into compatible aesthetic platforms.



TEMPERATURE MONITORING CAPABILITIES

While the PMS-DAP is a data-centric protocol, it is intrinsically linked to the device's thermal and operational sensors to contextualize archived events. The protocol continuously logs timestamped telemetry from the following critical subsystems: sapphire tip contact temperature (via NTC thermistors), coolant reservoir levels, TEC (Thermocouple) current draw, and laser bar pulse duration stability. In the event of a thermal excursion exceeding pre-set safety thresholds (e.g., tip temperature $> 5^{\circ}\text{C}$ for a 4°C setpoint), the protocol triggers an automated "Critical Event" flag within the archive. This flag captures 60 seconds of pre-event and 30 seconds of post-event telemetry at a sampling rate of 10 Hz. This capability ensures that any archived safety report is accompanied by immutable, high-resolution operational context, facilitating root-cause analysis during audits or competent authority inquiries.

PREMIUM COMPONENT ASSEMBLY

The hardware substrate for the PMS-DAP is a dedicated, tamper-evident industrial-grade micro-SD card (industrial pSLC, 32GB, -25°C to 85°C operating range) permanently seated on the main control board. This local storage is the primary vault for all post-market data before encrypted synchronization. The assembly includes a hardware secure element (ATEECC608A) for cryptographic key storage and digital signature generation, ensuring each data block is non-repudiable. Data is structured using an append-only, hash-chained log format (SHA-256), making retrospective alteration mathematically detectable. The module operates independently of the treatment delivery CPU, ensuring that even in the event of a main system fault, the surveillance archive remains intact and write-protected.

DETAILED PARAMETERS

The following table delineates the operational, security, and compliance parameters of the Post-Market Surveillance Data Archiving Protocol. These specifications are fixed at the firmware level and are not user-serviceable.

Parameter	Specification
-----------	---------------

Archive Storage Medium	Industrial pSLC micro-SD, 32GB, tamper-evident seal
Log Integrity Method	Append-only SHA-256 hash chain
Data Encryption Standard	AES-256-GCM (at rest and in transit)
Event Sampling Rate	10 Hz for critical telemetry; 1 Hz for routine logs
Pre/Post Event Buffer	60 seconds pre-event / 30 seconds post-event
Secure Element	Microchip ATECC608A (crypto authentication)
Synchronization Interval	Encrypted upload every 24 hours or upon Wi-Fi/Ethernet availability
Data Retention Period	Minimum 10 years (device lifecycle)
Regulatory Export Formats	FDA eSubmitter (3500A), EU MDR PSUR dataset (XML), ISO 14155 source data (CSV)

MEDICAL CERTIFICATIONS

The PMS-DAP has been designed and validated to support the clinic's compliance with the following regulatory frameworks:

EU MDR 2017/745, Annex III (Technical Documentation on Post-Market Surveillance) and Article 83 (Post-Market Surveillance System). The protocol generates the Periodic Safety Update Report (PSUR) dataset automatically at 12-month intervals.

FDA 21 CFR Part 803 (Medical Device Reporting). The protocol includes a guided MDR eSubmitter export function, pre-populating Form 3500A fields with archived device identification and event data.

ISO 14155:2020 (Clinical Investigation of Medical Devices) for source data archival in post-market clinical follow-up (PMCF) studies.

ISO 27001:2022 (Information Security Management) for data-at-rest and data-in-transit encryption (AES-256-GCM).

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: All patient-identifiable data fields are pseudonymized at the point of capture using a salted hash; the mapping table is stored separately under clinic-controlled access.

CLINICAL ENVIRONMENT

The PMS-DAP is indicated for integration into any OEM aesthetic platform operating firmware version 4.0 or higher. It is agnostic to the specific treatment modality (e.g., diode laser, IPL, RF) and functions purely as a data aggregation and archival layer. The protocol does not alter primary treatment parameters or safety interlocks. Clinics must designate a Data Protection Officer (DPO) or equivalent role to manage archive access credentials and perform the quarterly data integrity verification procedure outlined in the service manual. The archive is designed for a minimum 10-year retention period, aligning with the typical medical device lifecycle and EU MDR technical documentation retention requirements. Upon decommissioning of the device, the secure element can be physically extracted and archived as a permanent, legally admissible record of the device's post-market history.

