Medical CE & FDA Technical Compliance Register: Data Integrity Policy for 7-Year Archiving

CLINICAL SAFETY POSITIONING

The Data Integrity Policy for 7-Year Archiving establishes a mandatory, system-wide governance framework for all aesthetic device platforms manufactured by this OEM. This policy defines the technical and procedural controls required to ensure that patient treatment records, device operational logs, calibration histories, and clinical outcome data remain complete, consistent, and accessible for a minimum retention period of seven (7) years. The policy is engineered to satisfy the most stringent international regulatory expectations for electronic records and electronic signatures, including ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available). All device firmware and software architectures described herein are designed to enforce this policy by default, without reliance on operator intervention. This document serves as the authoritative compliance register for clinics, distributors, and regulatory auditors.



TEMPERATURE MONITORING CAPABILITIES

Data integrity in aesthetic devices extends beyond patient records to include environmental and operational parameters that may affect treatment safety and efficacy. The 7-Year Archiving Policy mandates continuous, tamper-evident logging of critical thermal and energy delivery metrics. Each treatment session generates an immutable audit trail capturing handpiece temperature, coolant flow status, fluence output, pulse duration, and cumulative energy delivered. These logs are time-stamped, cryptographically signed, and stored in non-volatile memory. Any deviation from pre-set safety thresholds triggers an automatic event flag that is permanently archived. The system supports real-time temperature monitoring at the sapphire tip and internal TEC junctions, with a sampling frequency of 10 Hz. All thermal data is retained for the full seven-year period and can be exported in encrypted, human-readable formats

for regulatory review.

PREMIUM COMPONENT ASSEMBLY

The hardware architecture underpinning this policy includes industrial-grade, secure storage modules (AES-256 encrypted solid-state drives) with a minimum rated endurance of 10,000 write cycles. Each device is equipped with a dedicated data integrity controller that operates independently of the main treatment processor, ensuring that logging functions remain active even during treatment pauses or system standby. The controller includes a real-time clock with battery backup, tamper-detection circuitry, and a write-once-read-many (WORM) logical partition for finalised records. Handpiece assemblies incorporate embedded memory chips that store unique identification, usage counters, and calibration data, all of which are automatically synchronised with the central archive. This design prevents record loss due to handpiece replacement or device servicing.

DETAILED PARAMETERS

The following parameter register defines the technical specifications that govern the 7-year archiving policy across all compatible device platforms. These parameters are fixed at the firmware level and are not user-adjustable

without authorised service credentials and a validated change-control procedure.

Parameter	Specification
Retention Period	7 years minimum from date of record creation or last modification
Storage Medium	AES-256 encrypted industrial SSD, WORM partition for finalised records
Audit Trail Scope	All treatment parameters, thermal logs, user actions, calibration events, and system errors
Time-Stamping	Cryptographically signed, NTP-synchronised, battery-backed RTC
Data Export Format	Encrypted PDF/A-3 and XML with digital signature
Access Control	Role-based authentication, unique user IDs, automatic session lockout
Backup Frequency	Continuous local journaling; optional daily encrypted off-site backup
Tamper Evidence	Hardware tamper detection, write-once logs, checksum verification

	on export
Regulatory Alignment	21 CFR Part 11, EU MDR 2017/745, ISO 13485, IEC 62304, GDPR
Data Integrity Standard	ALCOA+ principles enforced by system design

MEDICAL CERTIFICATIONS

The Data Integrity Policy for 7-Year Archiving has been designed to support compliance with the following regulatory frameworks and standards: IEC 62304 (Medical Device Software Lifecycle), ISO 13485 (Quality Management Systems), ISO 14971 (Risk Management), 21 CFR Part 11 (Electronic Records; Electronic Signatures), EU GDPR (Data Protection), and FDA Guidance on Data Integrity and Compliance with Drug CGMP. The policy also aligns with the requirements of the Medical Device Regulation (EU MDR 2017/745) for post-market surveillance data retention. Certificates of conformity and audit reports are available upon request. The manufacturer maintains a validated quality management system that covers all archiving processes, including data backup, restoration, and migration procedures.

CLINICAL ENVIRONMENT

Implementation of this policy requires that the clinical environment provide a stable power supply (UPS recommended) and network connectivity for optional cloud-based backup. The device operates independently of network availability for local archiving; however, clinics are advised to schedule periodic encrypted exports to a secure off-site location. The system provides automated alerts for storage capacity, backup failures, and tamper events. A dedicated data protection officer should be appointed within the clinic to oversee access controls and audit trails. Training on data integrity procedures is mandatory for all operators and is available through the manufacturer's certified training portal. The 7-year retention period begins at the date of patient treatment or device log generation, whichever is later, and is enforced by the system's internal calendar.

