Prepared By	Reviewed By	Approved By
Gitanjali Pawar	**Pramod Biradar**	**Umesh kalan**
(QA Engineer)	**(Manufacturing HOD)**	**(QA HOD / MR)**

1.0 PURPOSE

To establish and maintain Good Documentation Practices (GDP) and Data Integrity controls for all documents and records generated, maintained, reviewed, approved, stored, retrieved and retained as part of the Quality Management System (QMS).

This SOP ensures that quality-related information and records are:

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate
- Complete
- Consistent
- Enduring
- Available
- Traceable
- Secure and protected against unauthorised alteration or deletion

The procedure applies to both **paper-based and electronic records** and supports compliance with ISO 13485:2016, Medical Devices Rules, 2017 and Regulation (EU) 2017/745.

2.0 SCOPE

This SOP applies to all personnel and departments involved in creation, recording, review, approval, processing, correction, storage, retrieval, retention or disposal of QMS documents and records.

This includes, as applicable:

1. Quality Assurance
2. Quality Control

3. Production
4. Stores
5. Purchase
6. Engineering
7. Maintenance
8. Research and Development
9. Regulatory Affairs
10. Service
11. Human Resources
12. Information Technology
13. Suppliers and outsourced processes, where applicable

This SOP covers:

- SOPs
- Work Instructions
- Specifications
- Drawings
- Forms and formats
- Batch/Manufacturing records
- Inspection records
- Testing records
- Calibration records
- Validation records
- Verification records
- CAPA records
- NCR records
- Complaint records
- Audit records
- Training records

- Environmental monitoring records
- Risk-management records
- Technical documentation records
- PMS/vigilance records
- Electronic records
- Computer-generated data
- Raw data
- Audit trails
- Other QMS records

3.0 REFERENCES

3.1 External References

1. ISO 13485:2016 – Medical devices – Quality management systems – Requirements for regulatory purposes
2. Medical Devices Rules, 2017 – Fifth Schedule – Quality Management System
3. Regulation (EU) 2017/745 on Medical Devices
4. Applicable CDSCO requirements
5. Applicable European Union regulatory requirements
6. Applicable product-specific standards
7. Applicable customer and statutory requirements

Indian MDR 2017's Fifth Schedule establishes QMS requirements for medical-device manufacturers, including documentation and control of records.

EU MDR Article 10(9) requires manufacturers to establish, document, implement, maintain, update and continually improve a QMS proportionate to the risk class and type of device.

4.0 DEFINITIONS

4.1 Document

Information and its supporting medium used to specify requirements, instructions, methods or processes.

4.2 Record

Documented evidence that an activity has been performed or a result has been achieved.

4.3 Good Documentation Practices (GDP)

Practices established to ensure that documents and records are created, completed, corrected, reviewed, approved, stored and retained in a controlled and reliable manner.

4.4 Data Integrity

The completeness, consistency, accuracy, reliability and trustworthiness of data throughout its entire lifecycle.

4.5 ALCOA

ALCOA means:

- **A – Attributable**
- **L – Legible**
- **C – Contemporaneous**
- **O – Original**
- **A – Accurate**

4.6 ALCOA+

ALCOA+ additionally includes:

- Complete
- Consistent
- Enduring
- Available

4.7 Raw Data

Original information generated during an activity, measurement, inspection, testing or process.

4.8 Original Record

The first record in which data is captured or an authorised verified true copy of the original.

4.9 True Copy

A copy of an original record that has been verified and documented as an exact and complete representation of the original.

4.10 Data Lifecycle

The complete period from creation/generation of data through processing, review, reporting, storage, retrieval, archival and final disposal.

4.11 Audit Trail

A secure, computer-generated record that allows reconstruction of activities or changes to electronic data.

5.0 RESPONSIBILITIES

5.1 Quality Assurance

QA shall:

1. Establish and maintain this SOP.
2. Ensure implementation of GDP requirements.
3. Approve controlled documents and formats.
4. Monitor compliance with GDP.
5. Review quality records where required.
6. Conduct periodic documentation audits.
7. Review data-integrity incidents.
8. Ensure appropriate investigation and CAPA.
9. Ensure obsolete documents are withdrawn from points of use.
10. Ensure records are retained as per applicable requirements.
11. Provide GDP and Data Integrity training.
12. Ensure applicable regulatory requirements are incorporated into the QMS.

5.2 Department Head

Department Heads shall:

1. Ensure employees follow this SOP.
2. Ensure records are completed correctly.
3. Review records for completeness and accuracy.
4. Ensure only approved documents and forms are used.
5. Ensure documentation errors are appropriately corrected.
6. Immediately report suspected data-integrity issues to QA.

5.3 Employees / Record Generators

Employees shall:

1. Record data at the time of activity.
2. Record actual observations and results.

3. Make entries clearly and legibly.
4. Sign/initial and date records as applicable.
5. Use only current approved documents.
6. Correct errors according to this SOP.
7. Protect records from damage or unauthorised access.
8. Report documentation errors and suspected data-integrity violations.

5.4 IT / System Administrator

Where applicable, IT/System Administrator shall:

1. Maintain controlled user access.
2. Maintain individual user IDs.
3. Control passwords and access rights.
4. Maintain electronic backup.
5. Support data recovery.
6. Protect electronic records from unauthorised access.
7. Support audit-trail and system-security requirements.
8. Maintain relevant system administration records.

6.0 PROCEDURE

6.1 GENERAL GDP REQUIREMENTS

All QMS documents and records shall be:

- Clear
- Legible
- Accurate
- Complete
- Traceable
- Contemporaneous
- Permanent
- Retrievable
- Protected

- Controlled

Records shall be generated at the time the activity is performed.

No person shall intentionally create, modify, conceal, delete or destroy information in a manner that may compromise data integrity.

6.2 ALCOA+ REQUIREMENTS

All applicable quality records shall follow ALCOA+ principles.

Principle	Requirement
Attributable	Record shall identify who performed the activity and/or made the entry.
Legible	Record shall be readable and understandable.
Contemporaneous	Data shall be recorded when the activity is performed.
Original	Original data or verified true copy shall be retained.
Accurate	Data shall represent the actual activity/result.
Complete	Required information, including relevant changes, shall be retained.
Consistent	Date, time, sequence and records shall be logical and consistent.
Enduring	Records shall remain readable and protected throughout retention.
Available	Records shall be readily retrievable when required.

6.3 DOCUMENT ENTRY REQUIREMENTS

The following requirements shall be followed:

1. Use only approved formats.
2. Use permanent and indelible ink for paper records unless otherwise specified.
3. Write clearly and legibly.
4. Record actual results.
5. Record entries immediately after performing the activity.
6. Use approved units of measurement.
7. Use approved date and time formats.
8. Sign/initial entries as applicable.
9. Do not leave required fields blank.
10. Enter **N/A** where a field is genuinely not applicable.
11. Do not pre-fill records.
12. Do not pre-sign records.
13. Do not sign for another person.
14. Do not use correction fluid.

15. Do not erase original entries.

6.4 RECORDING OF ACTUAL RESULTS

The actual observed/measured result shall be recorded.

For example:

If the instrument displays:

3.96 V

the record shall contain:

3.96 V

It shall not be changed to an expected value such as **4.00 V**.

Failed, out-of-specification or unexpected results shall not be concealed or deleted.

Any investigation, retest or repeat test shall be performed and documented according to the applicable procedure.

6.5 DATE AND TIME

Date and time shall be recorded according to the approved organisational format.

Example:

Date: 11/08/2026
Time: 14:30

Entries shall reflect the actual date and time of the activity.

Backdating or falsely dating records is prohibited.

6.6 SIGNATURE AND INITIAL CONTROL

Signatures/initials shall be attributable to the individual performing or reviewing the activity.

The organisation shall maintain an authorised signature/initial record where required.

Personnel shall not:

- Sign for another person
- Share signatures
- Pre-sign blank records
- Allow another person to use their signature
- Use another person's credentials

Electronic signatures shall be uniquely attributable to the authorised user.

6.7 CORRECTION OF PAPER RECORDS

When an error is identified:

1. Draw a single line through the incorrect information.
2. Ensure the original information remains readable.
3. Enter the correct information near the original entry.
4. Provide the reason for correction where required.
5. Add signature/initial.
6. Add date of correction.

Example:

Incorrect:

Correct:

25.5°C / Wrong entry / MS / 11.08.2026

The original entry shall remain visible.

6.8 PROHIBITED CORRECTION METHODS

The following are strictly prohibited:

- Erasing
- Overwriting
- Correction fluid
- Scratching out original information
- Removing pages without authorisation
- Covering original information
- Backdating
- Falsifying records
- Concealing failed results
- Destroying original data

6.9 BLANK FIELDS

Required fields shall not be left blank without justification.

Where information is not applicable, enter:

N/A

Unused lines or spaces shall be controlled as defined in the applicable form/procedure.

6.10 RAW DATA CONTROL

Raw data generated during manufacturing, inspection, testing, calibration, validation, verification or other quality activities shall be retained as applicable.

Examples:

- Instrument readings
- Test results
- Instrument printouts
- Electronic files
- Photographs
- Measurement data
- Calibration data
- Validation data
- Verification results
- Computer-generated reports

Raw data shall not be discarded merely because the final result has been transferred to another record.

6.11 TRUE COPY

Where an original record is copied, the copy shall be verified as a true and complete representation of the original.

The verification shall include, as applicable:

- Comparison with original
- Identification of verifier
- Date
- Signature/initial
- Identification of the original record

6.12 ELECTRONIC RECORDS

Electronic records shall be controlled throughout their lifecycle.

Controls shall include, as applicable:

1. Unique user identification.
2. Password-controlled access.
3. Role-based access.
4. Authorised access only.
5. Periodic review of access rights.
6. Audit-trail controls where applicable.
7. Backup and recovery.
8. Protection against unauthorised modification/deletion.
9. Data retention.
10. Data retrieval.
11. System security.
12. Appropriate validation/verification of computerised systems.

Indian MDR 2017 specifically requires that, where documentation is handled electronically, authorised persons enter or modify data, changes and deletions are recorded, access is restricted, critical data entry is independently checked, electronic batch records are backed up and relevant data remains available during retention.

6.13 USER ACCESS CONTROL

Each authorised user shall have an individual user ID where the system requires user accountability.

User access shall be based on job responsibilities.

Access shall be removed or modified when:

- Employee leaves the organisation.
- Employee changes department.
- Employee changes responsibilities.
- Access is no longer required.

Shared accounts shall not be used where individual attribution is required.

6.14 PASSWORD CONTROL

Users shall:

- Keep passwords confidential.
- Not share passwords.
- Not write passwords in publicly accessible locations.
- Change passwords according to applicable IT requirements.
- Immediately report suspected password compromise.

6.15 AUDIT TRAIL

Where an electronic system has audit-trail functionality, the audit trail shall be enabled and protected where applicable.

The audit trail should allow reconstruction of relevant changes, including:

- Who made the change
- What was changed
- When the change was made
- Original information
- New information
- Reason for change, where required

Audit trails shall not be disabled, deleted or manipulated without authorised and documented justification.

6.16 COMPUTER SYSTEM VALIDATION / VERIFICATION

Computerised systems used for quality, production, monitoring, measurement, testing or regulatory activities shall be assessed for suitability.

Where required based on intended use and risk, the system shall be:

- Validated or verified
- Controlled
- Maintained
- Protected
- Backed up
- Subject to change control

System changes affecting data integrity shall be evaluated and controlled.

6.17 DOCUMENT CONTROL

Documents required by the QMS shall be controlled through the applicable Document Control SOP.

The following shall be controlled:

1. Document number
2. Document title
3. Revision number
4. Effective date
5. Approval
6. Distribution
7. Revision history
8. Current revision status
9. Obsolete status

Only the current approved revision shall be available at the point of use.

Indian MDR 2017 requires QMS documents to be controlled and appropriately reviewed, approved, updated and identified by revision status.

6.18 OBSOLETE DOCUMENTS

Obsolete documents shall:

1. Be removed from points of use.
2. Be identified as obsolete where retained.
3. Be prevented from unintended use.
4. Be retained where required for traceability or regulatory purposes.

6.19 RECORD CONTROL

Records shall be:

- Identified
- Legible
- Protected
- Stored appropriately
- Easily retrievable
- Retained for the specified period

- Protected against loss or damage
- Disposed of in an authorised manner

Record retention shall be defined by applicable QMS, regulatory, statutory and customer requirements.

6.20 DATA SECURITY AND BACKUP

Electronic records shall be protected against:

- Unauthorised access
- Unauthorised modification
- Accidental deletion
- Data loss
- Data corruption
- Hardware failure
- Software failure

Backup shall be performed according to the applicable IT Backup Procedure.

Backup restoration shall be tested periodically where required.

6.21 DATA INTEGRITY THROUGHOUT DATA LIFECYCLE

Data integrity controls shall be applied during:

Data Generation → Recording → Processing → Review → Approval → Reporting → Storage → Retrieval → Archival → Disposal

At every stage, data shall remain complete, accurate, traceable and protected.

6.22 DATA INTEGRITY INCIDENT

A data-integrity incident includes, but is not limited to:

- Falsification of results
- Backdating
- Unauthorised modification
- Unauthorised deletion
- Concealing original results
- Sharing user credentials
- Signing for another person

- Deleting failed results
- Manipulation of electronic data
- Unauthorised alteration of records
- Destruction of original raw data
- Bypassing electronic controls

Any suspected incident shall be immediately reported to QA.

6.23 DATA INTEGRITY INCIDENT INVESTIGATION

QA shall evaluate the incident and determine:

1. What happened?
2. When did it happen?
3. Which record/system was affected?
4. Who performed the activity?
5. Whether the original data is available.
6. Whether product quality is affected.
7. Whether other batches/products/records are affected.
8. Whether regulatory requirements are affected.
9. Whether CAPA is required.

Where required, the investigation shall be managed through the applicable NCR/CAPA procedure.

6.24 REVIEW OF RECORDS

Records shall be reviewed by authorised personnel as defined in the applicable procedure.

The reviewer shall verify:

- Correct document revision
- Completeness
- Legibility
- Actual results
- Correct calculations
- Correct date/time
- Signatures/initials

- Corrections
- Attachments
- Acceptance criteria
- Product/batch/lot identification
- Traceability
- Required approvals

6.25 DOCUMENTATION OF FAILED / NON-CONFORMING RESULTS

Failed or non-conforming results shall be recorded as obtained.

The original result shall not be deleted or replaced.

Where investigation/retesting is required, the activity shall be performed under the applicable approved procedure and all original and subsequent results shall remain traceable.

6.26 DOCUMENTATION FOR PRODUCT TRACEABILITY

Records required for product traceability shall contain sufficient information to establish, as applicable:

- Product identification
- Batch/Lot number
- Serial number
- Component/part identification
- Date of manufacture
- Inspection/testing status
- Personnel involved
- Equipment used
- Relevant supplier information
- Release status

The level of traceability shall be based on applicable regulatory, product and QMS requirements.

6.27 QUALITY RECORD RETENTION

Records shall be retained for the period defined by the applicable:

- ISO 13485 requirements

- Indian MDR requirements
- EU MDR requirements
- Product-specific regulatory requirements
- Customer requirements
- Legal/statutory requirements

Where different requirements apply, the applicable regulatory requirement shall be evaluated and the longer period shall be used where appropriate.

For EU MDR, manufacturers must retain technical documentation and other specified documentation for the periods prescribed by Article 10; the applicable retention requirement shall be determined according to device type and regulatory status.

6.28 CONFIDENTIALITY AND PROTECTION OF RECORDS

QMS and regulatory records shall be protected from unauthorised access.

Access to confidential records shall be limited to authorised personnel.

Where records contain personal or commercially sensitive information, applicable privacy, confidentiality and information-security requirements shall be followed.

6.29 SUPPLIER / OUTSOURCED PROCESS RECORDS

Where quality-related activities are outsourced, relevant records shall be controlled and retained according to applicable supplier-quality and QMS requirements.

Supplier records shall remain traceable to the applicable:

- Supplier
- Purchase order
- Product/component
- Lot/batch
- Test/inspection
- Certificate/report

6.30 TRAINING

Personnel involved in QMS documentation shall receive training on:

1. GDP
2. Data Integrity
3. ALCOA+

4. Document Control
5. Record Control
6. Electronic Records
7. Data Integrity Incident Reporting
8. Applicable regulatory requirements

Training shall be completed before personnel independently perform activities requiring GDP compliance.

Retraining shall be provided when:

- SOP is revised
- Significant documentation errors occur
- Data-integrity issues occur
- New systems are introduced
- Regulatory requirements change

6.31 INTERNAL AUDIT / COMPLIANCE MONITORING

QA shall periodically evaluate GDP and Data Integrity compliance through:

- Internal audits
- QMS audits
- Record reviews
- Process audits
- Electronic-system reviews
- Data-integrity assessments
- Training effectiveness checks

Findings shall be managed through the applicable NCR/CAPA process.

7.0 DO'S AND DON'TS

7.1 DO'S

Sr. No.	DO
1	Record data immediately after performing the activity
2	Use approved forms
3	Record actual results
4	Use legible handwriting
5	Sign and date records
6	Maintain original/raw data
7	Correct errors using approved GDP method
8	Protect electronic records
9	Report errors immediately
10	Maintain traceability

7.2 DON'TS

Sr.	DON'T
1	Do not erase entries
2	Do not use correction fluid
3	Do not overwrite entries
4	Do not backdate
5	Do not falsify data
6	Do not pre-sign records
7	Do not share passwords
8	Do not sign for another person
9	Do not delete failed results
10	Do not use obsolete forms

8.0 RECORDS

The following records shall be maintained as applicable:

Sr.	Record	Responsibility
1	GDP Training Record	QA / HR
2	GDP Documentation Error Record	QA
3	Data Integrity Incident Record	QA
4	Record Review Checklist	Concerned Department / QA
5	Electronic Access Control Record	IT
6	Backup Record	IT
7	Audit Trail Review Record	QA / IT
8	Data Integrity Investigation Record	QA
9	CAPA Record	QA
10	Document/Record Retention Register	QA

9.0 FORMS / FORMATS

Sr. No.	Form / Format	Form No.
1	GDP Documentation Error Record	INV/SOP/QA/004/F1
2	Data Integrity Incident Report	INV/SOP/QA/004/F2
3	GDP Record Review Checklist	INV/SOP/QA/004/F3
4	GDP & Data Integrity Training Record	INV/SOP/QA/004/F4
5	Electronic Access Control Record	INV/SOP/QA/004/F5
6	Audit Trail Review Record	INV/SOP/QA/004/F6

10.0 COMPLIANCE / REQUIREMENT MAPPING

Requirement	Applicable Clause / Requirement	SOP Section
ISO 13485:2016	Document and record control	6.17, 6.19
ISO 13485:2016	Control of QMS documents	6.17–6.18
ISO 13485:2016	Control and retention of records	6.19, 6.27
ISO 13485:2016	Personnel competence/training	6.30
ISO 13485:2016	Monitoring/auditing of QMS	6.31
Indian MDR 2017	QMS documentation	3.0, 6.17
Indian MDR 2017	Control of records	6.19
Indian MDR 2017	Electronic data controls	6.12–6.16
Indian MDR 2017	Electronic backup and availability	6.12, 6.20
EU MDR 2017/745 Article 10(9)	Documented and maintained QMS	1.0, 2.0, 6.17
EU MDR 2017/745 Article 10	Technical documentation and records	6.10, 6.27
EU MDR 2017/745 Annex IX	QMS documentation/procedures/records	3.0, 6.17, 6.19
EU MDR 2017/745	PMS/Vigilance/CAPA documentation	6.22–6.23, 8.0

EU MDR Article 10(9) specifically requires the manufacturer's QMS to cover the organisation's quality processes and procedures, including regulatory compliance, risk management, product realisation, PMS, vigilance, CAPA, monitoring and data analysis.

EU MDR Annex IX requires the manufacturer to establish, document and implement the QMS and maintain its effectiveness throughout the device lifecycle.

11.0 REVISION HISTORY

Revision No.	Effective Date	Description of Change	Prepared By	Approved By
00	01.09.2026	Initial Issue		