PQS Data Integrity Self-Assessment Checklist

Practical educational worksheet for pharmaceutical quality systems, laboratories, manufacturing and computerized records

Site / Department:		Assessment date:	
System / Process:		Assessor:	
Scope / Record type:		Reference SOP(s):	

1. Governance and data-lifecycle controls

Check	Assessment question	Status / evidence
[ ]	Are data-integrity responsibilities defined across users, reviewers, system owners, Quality Unit and management?	[ ] Yes [ ] No [ ] N/A
[ ]	Is the scope of GMP/GxP data understood, including paper, electronic, hybrid, metadata and temporary data?	[ ] Yes [ ] No [ ] N/A
[ ]	Are procedures in place for generation, processing, review, reporting, retention, archival and retrieval?	[ ] Yes [ ] No [ ] N/A
[ ]	Are data-integrity controls based on data criticality, process understanding and system risk?	[ ] Yes [ ] No [ ] N/A
[ ]	Are training and periodic awareness activities appropriate to role and system risk?	[ ] Yes [ ] No [ ] N/A
[ ]	Can the organization reconstruct the complete evidence behind a quality decision?	[ ] Yes [ ] No [ ] N/A

2. Lifecycle gate review

Gate	Key question	Evidence / concern
Generate	Is the first capture controlled, attributable and contemporaneous?	
Record / Process	Can calculations, transformations, changes and processing be reconstructed?	
Review	Does review cover the complete record required for the quality decision?	
Report / Decide	Does the final report faithfully represent the full evidence?	
Retain / Archive	Will data remain complete, readable and secure throughout retention?	
Retrieve	Can archived data and relevant metadata be restored when needed?	

PQS Data Integrity Self-Assessment Checklist

3. ALCOA+ evidence matrix

Principle	Evidence to verify	Status	Notes
Attributable	Unique identity/signature, date/time, traceable actions and appropriate user access.	[ ] Y [ ] N [ ] N/A	
Legible	Readable permanent records; electronic readability preserved throughout retention.	[ ] Y [ ] N [ ] N/A	
Contemporaneous	Entries and timestamps correspond to when the activity occurred.	[ ] Y [ ] N [ ] N/A	
Original / True Copy	Original record or verified true copy preserves content, meaning and relevant metadata.	[ ] Y [ ] N [ ] N/A	
Accurate	Verified calculations, controlled processing, calibrated/qualified systems and reviewed transcriptions.	[ ] Y [ ] N [ ] N/A	
Complete	All relevant passing, failing, repeated, aborted and changed records remain available.	[ ] Y [ ] N [ ] N/A	
Consistent	Chronology, IDs, sequence, records and timestamps tell the same story.	[ ] Y [ ] N [ ] N/A	
Enduring	Controlled durable storage, backup and archival preserve the record.	[ ] Y [ ] N [ ] N/A	
Available	Records can be retrieved with context for review, investigation and inspection.	[ ] Y [ ] N [ ] N/A	

Review principle: Do not assess ALCOA+ as nine isolated words. Ask whether the complete scientific and chronological story behind the decision can be reconstructed.

PQS Data Integrity Self-Assessment Checklist

4. Paper and hybrid records

Check	Control point	Status / evidence
[ ]	Controlled forms/worksheets are issued, identified and reconciled as required.	[ ] Y [ ] N [ ] N/A
[ ]	Entries are made directly in controlled records at the time of the activity.	[ ] Y [ ] N [ ] N/A
[ ]	Corrections preserve the original information and are attributable/traceable.	[ ] Y [ ] N [ ] N/A
[ ]	Unofficial scraps, notebooks or temporary worksheets are prevented or formally controlled.	[ ] Y [ ] N [ ] N/A
[ ]	Hybrid records preserve the relationship between paper output and underlying electronic/raw data.	[ ] Y [ ] N [ ] N/A

5. Electronic records, access and audit trails

Area	Assessment question	Status / evidence
User access	Are unique accounts, role-based privileges and periodic access reviews implemented?	[ ] Y [ ] N [ ] N/A
Admin access	Is privileged access limited, justified, logged and independently reviewed where appropriate?	[ ] Y [ ] N [ ] N/A
Audit trail	Are relevant changes, deletions, reprocessing and critical events captured and reviewed based on risk/procedure?	[ ] Y [ ] N [ ] N/A
Metadata	Are timestamps, user identity, method/sequence details and processing context retained where needed?	[ ] Y [ ] N [ ] N/A
Validation	Is the computerized system validated/verified as appropriate for intended GMP use?	[ ] Y [ ] N [ ] N/A
Backup	Are backups protected, tested and capable of restoring required records/context?	[ ] Y [ ] N [ ] N/A
Archival	Can retained data remain readable, accessible and linked to the original quality decision?	[ ] Y [ ] N [ ] N/A

PQS Data Integrity Self-Assessment Checklist

6. Scenario review

Scenario	Assessment	Your note
Shared HPLC account used by several analysts.	Attribution risk / red flag.	
Paper correction keeps original visible and follows approved correction procedure.	Generally acceptable control.	
Unfavorable injection is deleted; only passing repeat remains.	Serious completeness/data-integrity red flag.	
Repeat injection is scientifically justified, documented and both injections are retained.	Potentially acceptable under approved procedure.	
Release spreadsheet has editable formulas and no controlled version.	Accuracy/change-control red flag.	
Validated spreadsheet has protected formulas, access control and versioning.	Acceptable when fit for intended use.	

7. Six-question PQS risk triage

#	Question	Assessment / evidence
1	What quality decision did the data support?	
2	Can the original record and relevant metadata be reconstructed?	
3	Did system design, access, procedure or review weakness enable the event?	
4	What is the scope - one record/user/system or potentially broader?	
5	Could similar events have occurred without detection?	
6	Does the event affect product quality, patient risk or regulatory decisions?	

Escalation consideration: Missing/deleted raw data, inability to reconstruct data supporting a release decision, unexplained privileged access, intentional falsification indicators, or evidence of a broader systemic issue generally warrant prompt Quality Unit assessment under the site's approved procedures.

PQS Data Integrity Self-Assessment Checklist

8. Concern / event record

Concern identified:	
Date / time / source:	
Affected data / system / batch:	
Evidence preserved:	
Event reconstruction:	
Scope assessment:	
Product / quality impact:	
Root cause / contributing controls:	

9. Action plan

Action / CAPA	Owner	Due date	Effectiveness evidence

Final self-assessment:
[ ] Controls appear effective for the assessed scope
[ ] Improvement actions required
[ ] Formal deviation / investigation required
[ ] Quality Unit escalation required

Educational resource: This checklist does not replace approved company procedures, regulatory requirements, computerized-system validation, formal investigations, CAPA or Quality Unit decisions.