DATA INTEGRITY QUICK REFERENCE

ALCOA+ Principles

Principle	Meaning	Key Requirement
A	Attributable	WHO performed the action? Individual user ID required - no shared logins!
L	Legible	CAN data be read? Permanent, clear, retrievable throughout retention period
C	Contemporaneous	WHEN was it recorded? At the time of activity - no backdating!
O	Original	IS it the original? First capture or certified true copy
A	Accurate	IS it correct? Error-free, complete, reflects actual observation
+C	Complete	Is ALL data present? Including failures, repeats, deletions
+C	Consistent	Is data consistent? Timestamps, sequences, formats aligned
+E	Enduring	Is data protected? Retained for required period, backed up
+A	Available	Is data accessible? Retrievable when needed (inspections!)

KEY REGULATORY REFERENCES

FDA 21 CFR Part 11	Electronic Records & Signatures
EU GMP Annex 11	Computerised Systems
PIC/S PI 041-1	Good Practices for Data Management and Integrity
WHO TRS 1033 Annex 4	Guideline on Data Integrity

IMMEDIATE ACTIONS FOR COMPLIANCE

- Enable audit trails on ALL GxP systems - protect from modification
- Eliminate generic logins - create individual accounts for every user
- Review audit trails as part of batch release and periodically
- Train all staff on ALCOA+ and Good Documentation Practices
- Validate critical spreadsheets and protect with access controls

12 RED FLAGS - DATA INTEGRITY WARNING SIGNS

Based on 2024 FDA Inspection Findings - Investigate Immediately!

#	Red Flag	What to Look For
1	**Changes Outside Working Hours**	Data modifications at nights, weekends, holidays
2	**Changes Before Batch Release**	Multiple edits immediately before QA review
3	**Missing Reason for Change**	Audit trail changes without documented justification
4	**Test Repetitions w/o Investigation**	Multiple test runs, only passing results reported
5	**Deleted Data**	Any deletion without documented approval
6	**Sequence Gaps**	Missing sequence numbers in batch records/samples
7	**Backdated Entries**	System timestamp differs from recorded activity time
8	**Generic/Shared Logins**	Use of 'Lab', 'Admin', 'QC' shared accounts
9	**Timestamp Anomalies**	Time jumps, inconsistent sequences, out-of-order events
10	**Unusually Short Processing Times**	Activities completed faster than physically possible
11	**Audit Trail Gaps**	Periods with no entries despite expected activity
12	**Excessive Failed Logins**	Multiple failed attempts may indicate intrusion attempts

ESCALATION PATH

CRITICAL	Intentional falsification, fraud	Escalate to Site Director within 4 hours
MAJOR	Significant control gaps	Report to QA Manager within 24 hours
MINOR	Isolated incidents, documentation errors	Document, trend, address in 5 days

GOLDEN RULES OF DATA INTEGRITY

✓ Record data at time of activity	✗ Never backdate or pre-date entries
✓ Use your own login credentials	✗ Never share passwords or accounts
✓ Report all results including failures	✗ Never delete data without approval
✓ Make corrections with single strikethrough	✗ Never use white-out or overwrite
✓ Report concerns immediately	✗ Never ignore suspicious patterns