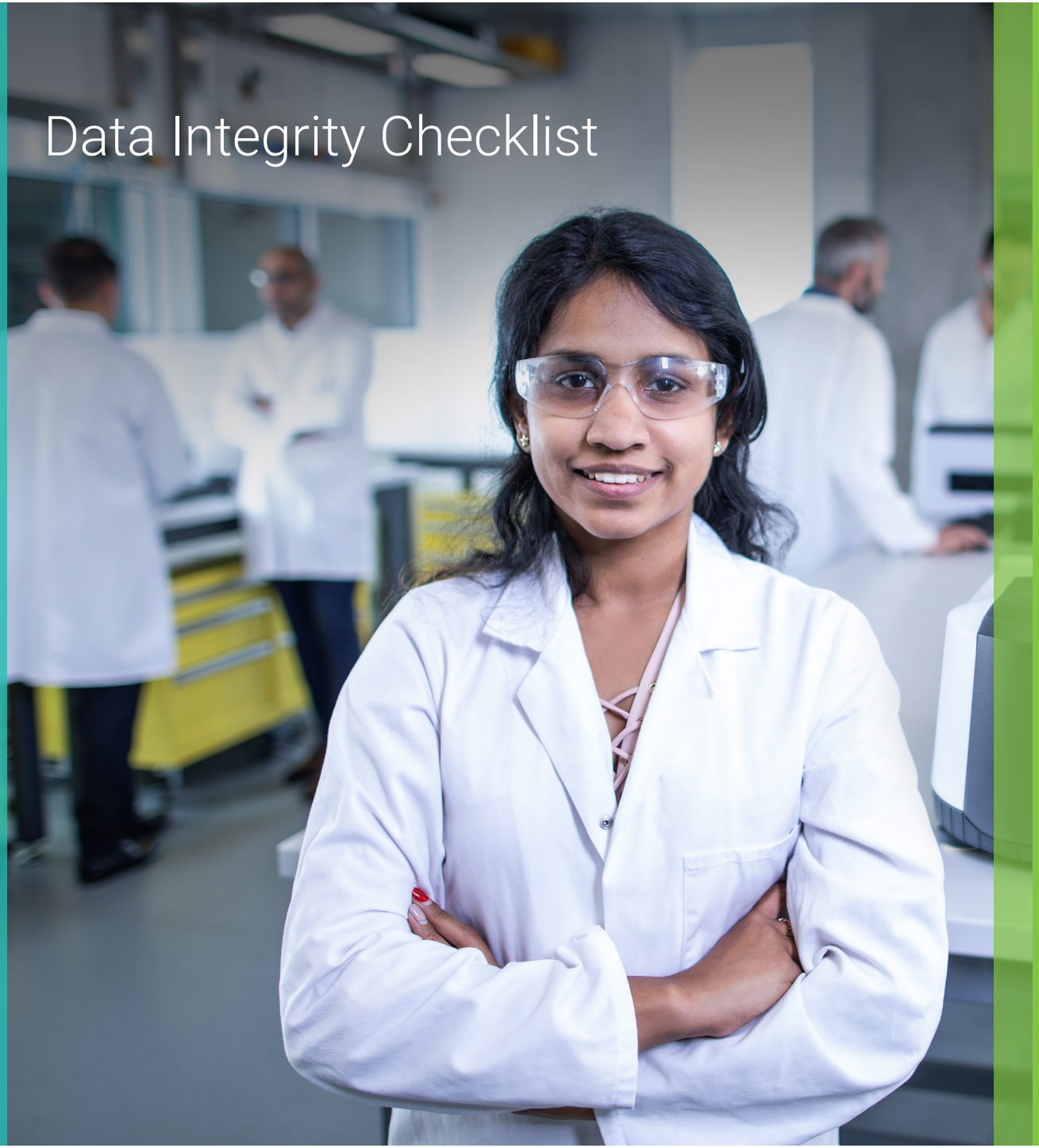
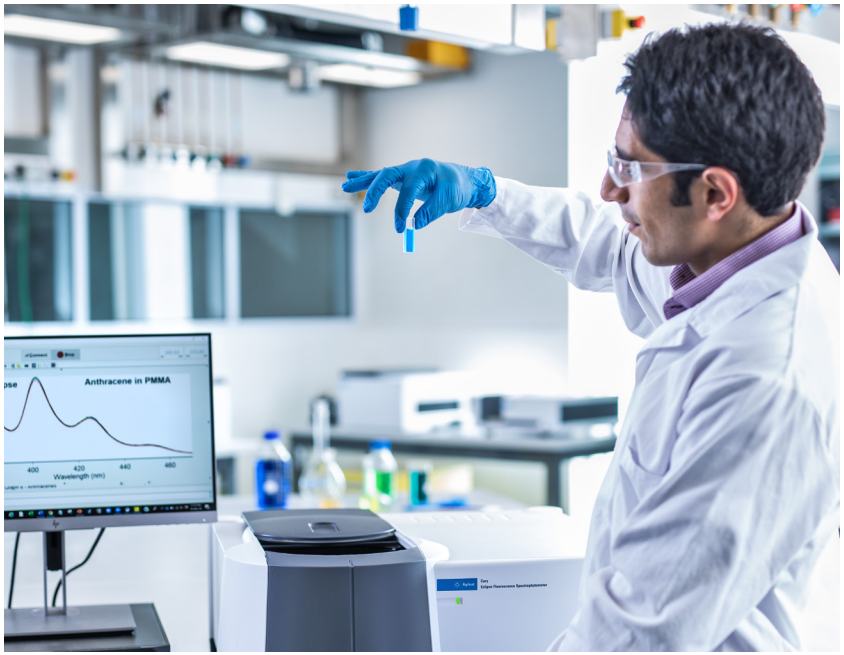
Data Integrity Checklist



Agilent

Trusted Answers

Data Integrity is defined as “the degree to which data are complete, consistent, accurate, trustworthy, and reliable and that these characteristics of the data are maintained throughout the data life cycle”. Data integrity is a fundamental requirement for an effective Pharmaceutical Quality System that ensures medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence and may ultimately undermine the quality of medicinal products (1).



The ALCOA principles for data integrity originated from the US Food and Drug Administration’s (FDA) Code of Federal Regulation for Good Laboratory Practice (GLP). These principles have since been expanded and renamed ALCOA+. A summary of the ALCOA+ principles is shown in the table, following. Detailed descriptions can be found in the Pharmaceutical Inspection Co-operation Scheme’s (PIC/S) guidance on Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments (1).

ALCOA+ principles for data integrity

A	**A**ttributable	The person collecting the data can be identified
L	**L**egible	Data must be readable and permanent
C	**C**ontemporaneous	Data must be recorded at the time it was generated
O	**O**riginal	Data is the source or primary data, not a copy
A	**A**ccurate	Data is truthful
C	**C**omplete	All required data is included in the record
C	**C**onsistent	Data is recorded and presented in the same format, in chronological order where relevant
E	**E**nduring	Data is maintained for its entire required retention period
A	**A**vailable	Data is accessible in a readable format during its retention period

Checklist

Use the checklist, following, to determine your level of compliance with ALCOA+ principles. This checklist is not exhaustive. You should also have systems and resources in place to determine your level of compliance with the data integrity requirements of the current good manufacturing practices (cGMPs) under which your facility operates.

Paper-based systems

		Confirmed	Notes
1.	Does your company maintain a signature log for employees that work in GxP areas?	☐	
2.	Are employees trained in Good Documentation Practices outlining that GxP records must be initialed and dated?	☐	
3.	Is the use of scribes prevalent in your company?	☐	
4.	When making a nonstandard entry (eg, empty field, changes to data), is a reason provided, along with the date and user's initials?	☐	
5.	Is data always recorded by the person generating or witnessing it – not someone they've asked to do it for them?	☐	
6.	Are digital images of a person's handwritten signature permitted at your company?	☐	
7.	Are controls in place to ensure data is recorded using permanent, blue, or black indelible ink?	☐	
8.	Is the use of correction fluid, pencils, and erasures prohibited?	☐	
9.	Is original data still readable when a correction has been applied?	☐	

		Confirmed	Notes
10.	Is there controlled issuance of bound, paginated notebooks for GMP activities?	☐	
11.	Are archiving of paper records performed by an independent, designated archivist?	☐	
12.	Are operators trained to use single-line crossouts accompanied by an initial and date when recording changes to a record?	☐	
13.	Are direct-printed paper records from equipment such as balances signed and dated? Do they include a reference to the sample ID or batch number?	☐	
14.	Are employees trained in Good Documentation Practices emphasizing the importance of recording data entries at the time of activity?	☐	
15.	Are employees trained in Good Documentation Practices emphasizing that it is wrong to backdate or forward date a record?	☐	
16.	Are sticky notes or other unofficial notepads permitted in GMP areas of the facility?	☐	
17.	Are qualification/validation activities performed on original pre-approved protocols?	☐	
18.	Is there a controlled and secure area for archiving records?	☐	
19.	Are original records readily available for inspection?	☐	
20.	Are forms, logbooks, and notebooks formatted to easily allow for the entry of correct data?	☐	

		Confirmed	Notes
21.	Are copies of printouts (e.g. of thermo-paper records) marked as 'copies' when attached to records?	☐	
22.	Are copies of original paper records controlled during their life cycle to ensure they are maintained as 'true copies'?	☐	
23.	Are procedures in place to independently review original paper records?	☐	
24.	Is data generated always recorded as it is found – even if it's not expected or is out of specification?	☐	
25.	Are deviations and out-of-specification results investigated?	☐	
26.	Are there policies and procedures in place to guide employees in reporting a data integrity breach? E.g., a Whistleblower policy. Are they encouraged to do so?	☐	
27.	Is data reported to the same number of decimal places as the specification or test methods indicate?	☐	
28.	Is a single result averaged from two or more data points recorded to one decimal place more than the specification to ensure overall accuracy?	☐	
29.	Is rounding done only on the final calculation result, not intermediate results?	☐	
30.	Are laboratory instruments calibrated and maintained at appropriate frequency?	☐	
31.	Is data always recorded in the required format? E.g., using the correct units and significant figures	☐	

		Confirmed	Notes
32.	Are secondary checks performed to check the accuracy of critical data?	☐	
33.	Are employees pressured or incentivized for meeting production targets, leading to compromised accuracy of records?	☐	
34.	Are there regular internal audits that include checking data integrity?	☐	
35.	Is there a retention policy and archiving procedure for paper records?	☐	

Electronic systems

		Confirmed	Notes
36.	Have you done a risk assessment of the data generated within your laboratory to determine which instruments/systems represent the greatest risk to patient safety if the data integrity was compromised?	☐	
37.	Are data integrity requirements included in user requirements specifications when purchasing equipment?	☐	
38.	Have all your laboratory instruments been validated to ensure the accuracy and reliability of the data?	☐	
39.	Does the system use unique user logins with electronic signatures?	☐	
40.	Do your critical computerized systems support different user access levels (roles)?	☐	
41.	Are employees trained on the fundamentals of data integrity which requires them to never disclose their username or passwords to other employees?	☐	
42.	Is the same login used by multiple employees, or are the ID and password written down and visible (e.g. on a sticky note) at a computer?	☐	
43.	Do your critical computerized systems have an inactivity logout?	☐	
44.	Are there audit trials in place recording the identity of operators entering, changing, confirming, or deleting data?	☐	

		Confirmed	Notes
45.	Does the system identify and record the person releasing or certifying the batches? Is an electronic signature used?	☐	
46.	Is your stored data checked periodically for readability?	☐	
47.	Has your organization tested their disaster recovery plan in terms of retrieving electronic data records, e.g., could you retrieve laboratory data after a cyberattack?	☐	
48.	Are audit trails convertible to an intelligible form?	☐	
49.	Can general users switch off the audit trail?	☐	
50.	Is archived data checked periodically for readability?	☐	
51.	Is data backed up in a manner permitting reconstruction of an activity?	☐	
52.	Is your stored data checked periodically for readability?	☐	
53.	Does your system automatically generate a timestamp when data is entered?	☐	
54.	Do electronic signatures contain an automatically generated timestamp?	☐	
55.	Are users able to change the timestamps applied to records?	☐	

		Confirmed	Notes
56.	Are general users able to gain access and change the system clock or time zone settings?	☐	
57.	Do all your systems use a secure database to store data?	☐	
58.	Is data saved to unauthorized storage locations such as USB sticks?	☐	
59.	Is there sufficient availability of user terminals at the location where a GxP activity takes place?	☐	
60.	Is it possible to print batch release records showing any data that has been changed since the original entry?	☐	
61.	Are your electronic signatures permanently linked to their respective record?	☐	
62.	Is the person processing the data able to influence what data is reported or how it is presented?	☐	
63.	Does the system prevent the deletion of original data?	☐	
64.	Is it possible to take screenshots and use snipping tools to manipulate data?	☐	
65.	Is metadata periodically reviewed?	☐	
66.	Do you have a process in place for the secondary review of data critical to product quality? E.g., an electronic workflow that includes a review by a second analyst.	☐	

		Confirmed	Notes
67.	If you are using paper or PDF reports as a data record, could you reconstruct the raw data set from electronic records at a future date? Data sets include all the records of analysis such as raw data, metadata, relevant audit trail and result files, software/system configuration settings specific to each analytical run, and all data processing runs (including methods and audit trails).	☐	
68.	Do interfaces contain built-in checks for the correct and secure entry and processing of data?	☐	
69.	Do your systems perform a check on the accuracy of critical data and configurations?	☐	
70.	Is a final, averaged result rounded to the same number of decimal places as the specification? Averaging should not be used to hide variability in the data spread, e.g., all replicate results should meet the specification results.	☐	
71.	Are systems periodically reviewed?	☐	
72.	Are computerized systems validated to demonstrate security and incorruptibility of data?	☐	
73.	Is archived data protected against unauthorized amendment?	☐	
74.	Do you have a data quality team (or responsible person) in your lab that works together to conduct/support investigations, identify system gaps, and drive the implementation of improvements?	☐	
75.	Is there a policy governing how long electronic records are kept?	☐	

References

1. Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments, Pharmaceutical Inspection Co-Operation Scheme, July 2021.

When data integrity controls fail

An FDA warning letter issued to an API manufacturer details failures by the manufacturer to prevent unauthorized access or changes to data. The letter also describes failures to have adequate controls to prevent manipulation and omission of data. It states: "Multiple analysts, testing multiple drugs, deleted unknown peaks without justification. These manipulations made the drugs appear to meet their specifications. Of concern, one of these unknown peaks was for a residual solvent known to be a genotoxic impurity".

Common problems with molecular spectroscopy in regulated laboratories

Agilent GxP experts report the several problems they commonly observe in regulated labs:

- Molecular spectroscopy testing is not considered a GxP activity
- Old hardware and software are used with no alternative available if they fail – potentially impacting product release
- Instruments not networked, on old operating systems and using old versions of instrument software that offer limited data integtrity controls
- Electronic raw data stored on the local PC and can be accessed via the operating system, permitting deletion or manipulation

The Agilent 3500 UV-Vis spectrophotometer is compatible with the Agilent OpenLab software suite of products. OpenLab provides technical controls to protect data integrity in regulated laboratories. The 3500 instrument has minimal moving parts and removes common sources of error in UV-Vis measurements, giving you greater confidence in your data.

Learn more at www.agilent.com/chem/cary3500uv-vis

Learn more:
www.agilent.com/chem/networked-uv-vis

Buy online:
www.agilent.com/chem/store

Get answers to your technical questions and access resources in the Agilent Community:
community.agilent.com

U.S. and Canada
1-800-227-9770
agilent_inquiries@agilent.com

Europe
info_agilent@agilent.com

Asia Pacific
inquiry_lsca@agilent.com

DE44481.889849537

Published in the USA, October 14, 2021
5994-3874EN

Agilent
Trusted Answers