GRRMDP

Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries

DATA INTEGRITY CHECKLIST

The Use of the checklist is to review and determine the level of compliance with ALCOA+ and ALCOA++ principles. This checklist may not be exhaustive but definitely covering almost all the points as per different guidelines. It is necessary to note that to have systems and resources in place to determine the level of compliance with the data integrity requirements of the current good manufacturing practices (cGMPs) under which the facility operates.

Some key concepts of GdocPs are summarised by the acronym ALCOA: Attributable, Legible, Contemporaneous, Original and Accurate. The following attributes can be added to the table: Complete, Consistent, Enduring and Available (ALCOA+). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.

DATA INTEGRITY CHECKLIST

ALCOA+ / ALCOA++ principles for data integrity

ALCOA++ is a set of principles and guidelines used in the life sciences and other regulated spaces. The acronym, which has expanded over the years (hence the pluses), represents ten key tenets for ensuring the integrity of data throughout its lifecycle.

	Principle	Description
A	Attributable	Data should be attributable to a source (human or program) that created, modified, or reviewed it. Actions like data entry, changes, approvals, and movements should be credited. With accountability, potential errors and discrepancies can be quickly corrected.
L	Legible	Data must be easily readable and understandable throughout their lifecycle. This includes maintaining consistent formatting in electronic records and avoiding abbreviations or other jargon that may introduce ambiguity. Legibility ensures accurate interpretation.
C	Contemporaneous	Data should be recorded in a timely manner, as soon as possible, after the event or observation occurred. This recording helps minimize the risk of information loss or distortion. It also supports accurate and reliable documentation for critical events.
O	Original	Data should be captured without alterations, manipulations, or unauthorized edits. Steps should be taken to avoid any unauthorized modifications that could compromise data accuracy or reliability. Original data provides a reliable, reusable source of information for analysis, audits, and regulatory compliance.
A	Accurate	Data must be complete and free from errors or omissions. It should reflect the true values, observations, or results obtained during data collection or processing. Accuracy ensures that the data can be trusted for decisions downstream.
+	Complete	All relevant data is captured, including any necessary metadata. Consistent Data recording practices are uniform and standardized across different systems, instruments, or operators. Enduring Data is preserved over time in accordance with retention requirements. Available Data can be retrieved when needed.
+	Traceable	Data can be tracked throughout its entire lifecycle.
	Consistent	Information should be created, processed, and stored in a logical manner that has a defined consistency. This includes policies or procedures that help control or standardize data (e.g. chronological sequencing, date formats, units of measurement, approaches to rounding, significant digits, etc.).
	Enduring	Records should be kept in a manner such that they exist for the entire period during which they might be needed. This means they need to remain intact and accessible as an indelible/durable record throughout the record retention period.
	Available	Records should be available for review at any time during the required retention period, accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections.

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
Paper Documents				
1.	Is Data Integrity Policy and SOP defined and available in the company?			
2.	Are team trained on the Data Integrity Policy and SOP?			
3.	Does company maintain specimen signature log for all employees?			
4.	Are employees trained in Good Documentation Practices outlining that GxP records must be initialled/signed and dated?			
5.	Is SOP available for preparation of master documents/procedures review and approval?			
6.	Is there an approved procedure for distribution and control of SOP and templates used to record data (master, control, logs, etc)			
7.	Are all the documents maintained with unique identification number and prepared reviewed, approved with signature and date of authorized personnel?			
8.	Is there an approved procedure for retrieval and recovery of process recorded formats?			
9.	How are the Master copy (in soft copy) stored to prevent from unauthorized or inadvertent changes?			
10.	How individual operators are identified, data entry formats and amendments to documents are recorded?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
11.	Is SOP available for retrieval, retention, archival and disposal of records?			
12.	Is there a procedure to check and ensure that current version of documents is available at the user department?			
13.	Is document issuances, retrieval are recorded?			
14.	Is the number of copies, type of copy distributed is recorded and monitored?			
15.	Is issuance of bound, paginated notebooks for GMP activities are controlled?			
16.	Is reconciliation of issued records maintained?			
17.	Are completed documents routinely reviewed for accuracy, authenticity and completeness?			
18.	Is the use of temporary recording practices in scrap paper/scribes/rough notes practiced?			
19.	Are controls in place to ensure that data is recorded using permanent indelible ink?			
20.	Is the use of correction fluid, pencils and erasures prohibited?			
21.	Is original data readable when there is a correction?			
22.	Are archiving of paper records performed by an independent, designated individual?			
23.	Is there a retention policy and archiving procedure for paper records?			
24.	How issuance of additional pages is controlled if there is any requirement of additional pages to complete the document?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
25.	Are operators trained to use single-line cross outs accompanied by an initial and date when recording changes to a record?			
26.	Are all employees trained in Good Documentation Practices emphasizing the importance of recording data entries at the time of activity?			
27.	Are employees trained in Good Documentation Practices emphasizing that it is improper to back date or forward date a record?			
28.	Are sticky notes or other unofficial note pads permitted in GMP areas of the facility?			
29.	Are qualification/validation activities performed on original pre-approved protocols?			
30.	Is there a controlled and secure area for archiving of records?			
31.	Are original records readily available for inspection?			
32.	Are forms, logbooks and notebooks formatted to easily allow for the entry of correct data?			
33.	Are the paper printout pH meters and balances printout during data acquisition as the original record retained?			
34.	Are copies of printouts (e.g. of thermo-paper records) marked as 'copies' when attached to records?			
35.	Is the data required to be created and maintained is controlled and cannot be modified without a record of the modification?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
36.	Are copies of original paper records controlled during their life cycle to ensure they are maintained as 'true copies'?			
37.	Are procedures in place to independently review original paper records?			
38.	Is data generated always recorded as it is found even if it's not expected or is out of specification?			
39.	Are handwritten entries made by the person who executed the task?			
40.	Is the handwritten entry is legible and clear?			
41.	Is the team trained not to use unknown symbols / abbreviation? e.g. use of ditto (") marks			
42.	Check correct pagination of the records and all page's present.			
43.	Are the relevant records available within the immediate areas in which they are used?			
44.	Check the records for entries made with ink which is not erasable or will not smudge and not filled with pencil prior to use of pen (overwriting)?			
45.	Any over writings are observed in records?			
46.	Are records checked for key entries and signed with date? (Particularly if steps occur over time, i.e. not just signed at the end of the page and/or process).			
47.	Verify the process for the handling of production records within processing areas to ensure they are readily available to the correct personnel at the time of performing the activity to which the record relates.			
48.	Are the numbered sets of blank forms issued as			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	appropriate and reconciled upon completion of all issued forms?			
49.	Are the numbered sets of blank forms (including, but not limited to, worksheets, laboratory notebooks, and master production and control records) issued and reconciled upon completion?			
50.	Are the incomplete or erroneous forms kept as part of the permanent record along with written justification for their replacement?			
51.	Is the use of scribes to record activity on behalf of another operator is practiced? Eg. an activity is performed by an operator but witnessed and recorded by a second person.			
52.	Do the records identify both the person performing the task and the person completing the record?			
53.	Verify secondary checks performed during processing were performed by appropriately qualified and independent personnel, e.g. production supervisor or QA.			
54.	Check that documents were reviewed by production and then quality personnel following completion of operational activities.			
55.	Check that the secondary reviews of data include a verification of any calculations used.			
56.	Are the original laboratory records, including paper and electronic records, reviewed by a second person to ensure that all test results are appropriately reported?			
57.	Is the process for supervisory (scribe)			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	documentation completion described in an approved procedure that specifies the activities to which the process applies?			
58.	Check original data to confirm that the correct data was transcribed for the calculation			
59.	Are deviations and out-of-specification results investigated?			
60.	Is data reported to the same number of decimal places as the specification or test methods indicate?			
61.	Is a single result averaged from two or more data points recorded to one decimal place more than the specification to ensure overall accuracy?			
62.	Is rounding done only on the final calculation result, not intermediate results?			
63.	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?			
64.	Are laboratory instruments calibrated at appropriate frequency and maintained? Records available?			
65.	Are complete data in laboratory records, which includes raw data, graphs, charts, and spectra from laboratory instruments are retained? Are Suspected or known falsification or alteration of records fully investigated under the CGMP quality system to determine the effect of the event on patient safety, product quality, and data reliability; and to determine the root cause; and to			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	ensure the necessary corrective actions are taken?			
66.	Are records available to operators at the point-of-use?			
67.	Is data always recorded in the required format? E.g., using the correct units and significant figures			
68.	Are all data of system suitability testing included in the record that is retained and subject to review?			
69.	Are employees pressured for meeting production targets, leading to compromised accuracy of records?			
70.	Is there a defined procedure for storage and recovery of records?			
71.	Are all records stored in a specified designated location with easy identification and traceability?			
72.	Is there a system to ensure that all relevant records related to GMP/GDP are stored for periods that meet GMP/GDP requirements?			
73.	Are there systems in place to protect records (e.g. pest control and sprinklers)?			
74.	Are the records protected from damage or destruction by fire, liquid, rodents, unauthorized personnel access? (Who may attempt to amend, destroy or replace records).			
75.	Are archived records (original record or a 'true copy') protected so that they cannot be altered or deleted without detection and protected against any accidental damage such as fire or pest?			
76.	Is there a system in place for the recovery of records in a disaster situation?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
77.	Does regular internal audits include checking data integrity?			
78.	Is compliance with the principles and responsibilities verified during periodic site audits of contract accepter? Does verification includes the review of procedures and data (including raw data and metadata, paper records, electronic data, audit trails and other related data) held by the contract accepter identified in risk assessment?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
Electronic Documents				
79.	Does the admin / IT SOP outlined user access process, routine access reviews, and backup/recovery/ restore process?			
80.	Does any appropriate arrangements exist for the restoration of the software/system as per its original validated state, including validation and change control information to permit this restoration.			
81.	Does the user SOP detail entering and modifying critical data? Paper vs. electronic records?			
82.	Are agreements in place with local IT or IT service providers?			
83.	Is there a list of approved authorized IT service providers?			
84.	Is the most recent audit report reviewed and checked if CAPAs have been addressed? Did the audit address data integrity / governance?			
85.	Is there a quality agreement in place with the service provider – does it address data governance expectations / assign and define responsibilities between the service provider, the IT department and or individual users?			
86.	Is the data governance system ensuring controls over the data lifecycle which are			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	commensurate with the principles of quality risk management?			
87.	Is the effective review of the data governance system demonstrate understanding regarding importance of interaction of company behaviours with organisational and technical controls? The outcome of the review is it communicated to senior management, and be used in the assessment of residual data integrity risk?			
88.	Does the service provider interact directly with users or is all communication through the IT department?			
89.	Does the contractual agreements state that GxP activities, including outsourcing of data management, should not be sub-contracted to a third party without the prior approval of the contract giver?			
90.	Have service providers been provided GMP/GDP and specifically data integrity training and are they familiar with the DI Policy?			
91.	Are personnel trained in detecting data integrity issues as part of a routine CGMP training program?			
92.	Does the training on computerized systems include validation of computerized systems for example, system security assessment, back-up, restoration,			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	disaster recovery, change and configuration management, and reviewing of electronic data and metadata, such as audit trails and logs, for each GxP computerized systems used in the generation, processing and reporting of data?			
93.	Are IT service providers permitted remote access to company computers? If yes, is access with or without prior specific user, or manager, permission each entry to a user's workspace or a computerized system serving a piece of production, laboratory or other GxP related activity / operation?			
94.	Where 'cloud' or 'virtual' services are used following points considered: • Understanding service provided, ownership, retrieval, retention and security of data • Physical location where the data is held, including the impact of any laws applicable to that geographic location • Availability of technical agreement or contract defining the responsibilities of the contract giver and acceptor and responsibilities for archiving and continued readability of the data throughout the retention period			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
95.	Does the Contract Givers ensure that data ownership, governance and accessibility are included in any contract/technical agreement with a third party?			
96.	Is there a computerized systems policy?			
97.	Is the computer system intended to be used for workflow, such as creation of an electronic master production and control record (MPCR), validated? Validating the workflow ensures that the intended steps, specifications, and calculations in the MPCR are accurate.			
98.	Are there appropriate controls to assure that changes to computerized MPCRs, or other records, or input of laboratory data into computerized records, can be made only by authorized personnel?			
99.	Does it require all computerized systems with GxP impact to be compliant with: 21 CFR part 11 (electronic records and electronic signatures)/ Annex 11 of the EU GMPs/Other standards**?** (define)			
100.	Are Computerized systems validated for their intended purpose? To ensure that the steps for generating the custom report accurately reflect those described in the data checking SOP and that the report output is consistent with the procedural steps for performing the subsequent review			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
101.	Is there a documented system in place that defines the access and privileges of users of systems?			
102.	Are digital images of a person's hand written signature permitted?			
103.	Is the risk assessment done of the data generated within laboratory to determine which instruments/systems represent the greatest risk to patient safety if the data integrity was compromised?			
104.	Are data integrity requirements included in user requirements specifications while purchasing equipment?			
105.	Is all laboratory instruments validated to ensure the accuracy and reliability of the data?			
106.	Does the system use unique user logins with electronic signatures?			
107.	Are the controls documented which are used to identify the specific person who signed the records electronically if electronic signatures are being used?			
108.	Does electronic signature or E-signature systems provide for "signature manifestations" i.e. a display within the viewable record that defines who signed it, their title, and the date (and time, if significant) and the meaning of the signature (e.g. verified or approved)?			
109.	Do critical computerized systems support different user access levels (roles)?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
110.	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?			
111.	Do critical computerized systems have an inactivity logout?			
112.	Is a list of authorized individuals and their access privileges for each CGMP computer system in use maintained?			
113.	System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) is not assigned to individuals with a direct interest in the data (data generation, data review or approval)			
114.	Is the computer system, such as a Laboratory Information Management System (LIMS) or an Electronic Batch Record (EBR) system, designed to automatically save after each separate entry?			
115.	Are there audit trials in place recording the identity of operators entering, changing, confirming or deleting data?			
116.	Review some of the changes performed – Is there a computerized audit trail for PROGRAMMING changes?			
117.	Is there a controlled (up-to-date, version number, page #s) list of GxP impact computerized systems? Does it describe: What the system does,			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	where it is installed (list of PCs on which it is installed and authorized users); current validated software version?			
118.	Does the system identify and record the person releasing or certifying the batches? Is an electronic signature used?			
119.	Are employees trained on the fundamentals of data integrity which requires them to never disclose their username or passwords to other employees?			
120.	Is archived data checked periodically for readability?			
121.	Is the disaster recovery plan in terms of retrieving electronic data records tested? e.g., retrieving laboratory data after a cyberattack?			
122.	Is the backup and recovery processes are validated and periodically tested?			
123.	Is the backup strategies for the data owners documented?			
124.	Are archive arrangements designed to permit recovery and readability of the data and metadata throughout the required retention period? Are archiving of electronic data process is validated?			
125.	In case of hybrid records storage is the references between physical and electronic records maintained such that full verification			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	of events is possible throughout the retention period?			
126.	Are data collection audit trails reviewed? At what frequency and by whom? Are they attached to the results reviewed by QP at release?			
127.	Are audit trails convertible to a generally intelligible form?			
128.	Can general users switch off the audit trail?			
129.	Does review of audit trail include • change history of finished product test results, • changes to sample run sequences, • changes to sample identification, and changes to critical process parameters?			
130.	Does the GxP systems provide for the retention of audit trails which reflect users, dates, times, original data and results, changes and reasons for changes (when required to be recorded), and enabling and disenabling of audit trails?			
131.	Does the routine review of GxP data and meta data include audit trails?			
132.	Does the personnel responsible for record review under CGMP review the audit trails?			
133.	Does the audit trail for a high performance liquid chromatography (HPLC) run include the user name, date/time of the run, the integration parameters used, and details of a			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	reprocessing, if any, including change justification for the reprocessing?			
134.	Does an audit trail include those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file)?			
135.	Do all systems use a secure database to store data?			
136.	Is there 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.			
137.	If paper or PDF reports are being used as a data record, is it possible to 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).			
138.	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.			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
139.	Are the processes designed to ensure that quality data required to be created and maintained cannot be modified? E.g. chromatograms are sent to long-term storage (archiving or a permanent record) upon run completion instead of at the end of a day's runs.			
140.	Are computerized systems validated to demonstrate security and incorruptibility of data?			
141.	Is there a policy governing how long electronic records are kept?			
142.	Are the data stored electronically in temporary memory before creating a permanent record?			
143.	Do the analysts know how to print an audit trail data? Are the users identified by name or as User 1, 2, 3 or are they all just "User"?			
144.	Does the audit trail explain in human readable form, what change was made and why. If it describes the change but not the reason – ask the analyst, separately their manager and separately the QP who released the batch – what the reasons are. In particular focus on deletions.			
145.	Are programming audit trails (changes to directories, file deletion, alteration, changes to metadata) reviewed? At what frequency and by whom?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	How the review is documented and to whom is the outcome reported. Do findings appear in the CAPA system?			
146.	Are users able to amend or switch off the audit trail? If a system administrator amends, or switches off the audit trail Is a record of that action retained?			
147.	Are the user name and passwords program specific or is a workstation accessed by entering a windows user name and password? NOTE: if yes, probably all users are entering on a single user name and if a workstation has several programs installed, access to those programs is not controlled once the workstation is open.			
148.	Who holds the administrator password and what privileges does it allow (e.g. is the laboratory manager able to delete files?) Is there a policy describing what the administration is allowed to do and how it is documented?			
149.	How are changes to programming, servers, and IT infrastructure managed? Is it by the company wide change control program or an IT change control? Is there QA / Quality Unit sign off			
150.	Check if drawing tools are disabled (might allow “whiting out” a “small” unwanted peak			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	on a chromatogram and wouldn't be seen on the printout			
151.	Are chromatograms sequential or are there numbers missing in the set?			
152.	Is there an SOP describing how integration of chromatograms is performed? Is auto-integrate the default? If manual integration is performed is the auto-integration also attached?			
153.	Are the integration parameters and set up printed out before performing the analysis?			
154.	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?			
155.	How and by whom is the system clock set? Can it be changed to show an earlier time of processing data?			
156.	Is there a written policy regarding trial injections as part of system suitability? Does it forbid the use of test samples? What is the policy for filing and reporting failing system suitability tests – before, during and / or after testing?			
157.	Is data deletion possible and how is recorded in the audit trail?			
158.	Is there a written definition as to what constitutes raw data and how that is backed up?			
159.	Is data backed up in a manner permitting			

DATA INTEGRITY CHECKLIST

Site:

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	reconstruction of an activity?			
160.	Does the system automatically generate a timestamp when data is entered?			
161.	Do electronic signatures contain an automatically generated time stamp?			
162.	Are users able to change the time stamps applied to records?			
163.	Are general users able to gain access and change the system clock or time zone settings?			
164.	Are memory sticks / thumb drives or other removable media allowed? Or is there a policy forbidding their use / drives sealed off / computers not fitted with USB ports? Is data saved to unauthorized storage locations such as USB sticks?			
165.	Is there sufficient availability of user terminals at the location where a GxP activity takes place?			
166.	What is the maximum time from QC results generation until review and approval / COA issuance? Is this covered by an SOP? Including for stability testing results?			
167.	How are COAs generated? Is the template locked? Can it be overwritten? Does it match the specifications?			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
168.	Is it possible to print out batch release records, showing any data that has been changed since the original entry?			
169.	Are excel files used for calculating QC results? Is there an SOP and are excel files validated and locked?			
170.	What provisions are in place (e.g. immediate signing and dating of printed copy with deletion of original data from template) to prevent changing data after calculation?			
171.	Are the Electronic worksheets used in automation like paper documentation version controlled and any changes in the worksheet is documented/verified appropriately?			
172.	Check a template – is there data stored in it and does the company overwrite previous data? – a known source of error			
173.	Is there an IT Disaster Recovery Plan and does it address data governance?			
174.	Is there a procedure for retiring computerized systems / software which ensures that raw data is preserved and can be reused for calculation verification if required? Over what period of time?			
175.	Are electronic signatures permanently linked to the irrespective record?			
176.	Does the person processing the data have the ability to influence what data is reported or how it is presented?			
177.	Does the system prevent deletion of original			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	data?			
178.	Is it possible to take screenshots and uses snipping tools to manipulate data?			
179.	Is metadata periodically reviewed?			
180.	Does metadata for a particular piece of data include a date/time stamp for when the data were acquired, a user ID of the person who conducted the test or analysis that generated the data, the instrument ID used to acquire the data, audit trails, etc.?			
181.	Do interfaces contain built-in checks for the correct and secure entry and processing of data?			
182.	Does the system perform a check on the accuracy of critical data and configurations?			
183.	Are systems periodically reviewed?			
184.	Are interfaces validated to demonstrate security and no corruption of data?			
185.	Is data transfer process (transferring data between different data storage types, formats, or computerized systems) validated?			
186.	Are the Data transfer/migration procedures validated?			
187.	Is archived data protected against unauthorized amendment?			
188.	Does the backup file contain the data (which includes associated metadata) and is in the original format or in a format compatible with the original format?			

DATA INTEGRITY CHECKLIST

Site:

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
189.	Do you have a data quality team (or responsible person) that works together to conduct/support investigations, identify system gaps, and drive the implementation of improvements?			
190.	Is a true copy of electronic data, including relevant metadata, for the purposes of review, backup and archival created?			
191.	Does the data and document retention arrangement ensure the protection of records from deliberate or inadvertent alteration or loss?			
192.	Is appropriate controls identified and implemented based on risk assessment for the existing systems do not meet current requirements?			
193.	Is effectiveness of the controls implemented evaluated through: • the tracking and trending of data • a review of data, metadata and audit trails (e.g. in warehouse and material management, production, quality control, case report forms and data processing); and routine audits and/or self-inspections, including data integrity and computerized systems			
194.	Are there any legacy systems which do not meet part 11 requirements for:			

DATA INTEGRITY CHECKLIST

Site:

_____

S. No.	Check Points	Tick Mark as applicable		Observation /Remarks
		Yes	No	
	i) Unique user name / password for each entry with automatic LOGOFF			
	ii) How long after leaving the workstation does it log out			
	iii) Is there a data and time stamped audit trail for each piece of software at the data collection level?			
	iv) Is there a data and time stamped audit trail for each piece of software at the programming level?			
	v) Is the audit trail enabled?			
195.	Is a data integrity risk assessment (DIRA) performed? (where the processes that produce data or where data is obtained are mapped out and each of the formats and their controls are identified and the data criticality and inherent risks documented)			

Remarks if any:

Inspector/Auditor Signature & Date

References Links

1. U.S. Food and Drug Administration, Data Integrity and Compliance With Drug CGMP: Questions and Answers; Guidance for Industry, FDA-2018-D-3984, 2018, https://www.fda.gov/media/119267/download.
2. Pharmaceutical Inspection Convention/Pharmaceutical Inspection Cooperation Scheme, Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments Draft (PI-041), 2021, https://picscheme.org/docview/4234.
3. European Medicines Agency, EMA Draft Guideline on Computerized Systems and Electronic Data in Clinical Trials, 2021, https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-electronic-data-clinical-trials_en.pdf.