Data Integrity Auditing Checklist / Guide			
Management Culture			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
Quality Manual, or equivalent documentaton, with Management commitment to good DI practices.	Policies to include a code of ethics and proper conduct to assure the reliability and completeness of data.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 5. Quality risk management to ensure good data integrity	
	Policies to include mechanisms for staff to report quality and compliance concerns to Management.		
Influence of company culture.	**Open Culture**: hierarchy can be challenged by subordinates, and full reporting of systemic and individual failure is a business expectation.	PIC/S Guidance - PI 041-1 (Draft 2), 10 Aug 2016, Item 6.1.2	
	Closed Culture: reporting failure or challenging a hierarchy is difficult.		
Management understanding of Direct and Indirect influences	Direct controls are usually part of written procedures and policies, generally covering complex or inconsistent processes with open ended and subjective outcomes.		
	Indirect influences on behavior should be understood and addressed, i.e., incentives for productivity that exceed the process capability of a system.		
Do Data Integrity processes include a Quality Risk Management (QRM) component?	QRM is essential to ensure that data and record control strategies are commensurate with the potential impact on product quality, patient safety, and related decision-making.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 5. Quality risk management to ensure good data integrity	
	Ensure that adequate resources are committed to data and record management.		

Data Integrity Auditing Checklist / Guide			
Management Culture			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
	Record and data integrity risks should be assessed, mitigated, communicated, and reviewed throughout the data life cycle.		
Data integrity Training	Personnel should be trained in data integrity policies and agree to abide by them. Management ensures that personnel are trained to understand and distinguish between proper and improper conduct, and are aware of potential consequences.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 8. Training in good data management	
	Key personnel (i.e., Managers, Supervisors, Quality Unit Personnel) receive specific training to prevent and detect data integrity issues. Subjects to include review of system configurations, review of data and metadata, review of audit trails, etc.		
	Training is completed at the time of hire for an individual and then periodically thereafter.		
Response to Data Integrity breaches.	Management must demonstrate vigilance in detecting issues, understand reasons behind lapses, conduct investigations of the issue, and implement corrective and preventative actions.	PIC/S Guidance - PI 041-1 (Draft 2), 10 Aug 2016, Item 6.1.6	

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
Laboratory Information Management Systems (LIMS)	In most instances, the LIMS provides oversight management of all Lab operations. This may include: • analytical methods repository • sample management • worksheet generation • review and retention of analytical results • final data evaluation and approval • In some cases, LIMS is linked to inventory management systems to indicate when material can be released for distribution		
	System must be validated to demonstrate that it functions as required. • Audit Trails active for all data • Users are identified and assigned appropriate system authorities (Analyst should not have the same authority as Data Reviewers) • Lab worksheets are sufficiently indexed to allow traceability • Analytical results are second person reviewed following upload or data entry		

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
	If LIMS is used for Sample Management, the following should be verified: • Samples identified to allow traceability through Lab operations • Sample storage requirements • Analyst assignments to perform specific tests • Analytical test completion and transfer to sample retention • All transactions should be Date/Time stamped along with individual performing the data entry		
	Generation of a Certificate of Analysis (COA) must include the following: • Sample identification • Analytical Test identification • Acceptable Specifications (this may be a range) • Actual Analytical Results • Pass / Fail Determination • Date, Time, and Signature of the appropriate individual with authority to approve analytical results • Signature event must be a “wet” signature or an electronic signature (compliant with Part 11)		
Chromatography Systems (i.e., HPLC, GC)	Presence of the system user, data reviewer, and system administrator is recommended during review of such systems. These should be the primary resources to demonstrate the use of the system.		

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
	In most instances, chromatography instruments will be networked through chromatography data software (CDS) such as the Empower 3 system provided by the Waters Corporation. • Determine the data transfer sequence from analytical instruments to the CDS. • Ensure that the full record, including metadata, is captured to prevent any lost data. • Specifically, evaluate the ability to change the record during these sequences (which should not be possible) and the presence of an Audit Trail to capture any changes.		
	The same evaluation should be completed for subsequent records transfer from the CDS to a LIMS network (if applicable).		
	Review configuration settings for the CDS: • User accounts have unique names and passwords; passwords are routinely required to be revised • User accounts system authorities are assigned at the appropriate level for the user's role (Analyst, Data Reviewer, System Administrator) • Verify specific functions that can be performed by each system authority level to ensure they are appropriate for the user • Audit Trail is permanently on; user cannot turn it off • Users cannot change the system Time/Date		

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
	Check common places for written evidence of shared passwords: • Under keyboard • Behind monitor • Desk drawers • Contents of trashcans • Post-It notes in various locations		
	Request the System Administrator to assist with review of data folders and files on the system. • Look for sequential capture of data files; aborted runs (with explanation), sequential files with same name (or slightly different names) • Look for separate folders not with the formal data records; check for data files hidden with these folders • Verify Date and Time on data files • Verify that data files align with instrument use logs • Check the contents of the Trash Can		
Stand Alone Systems (vs. networked systems)	There may be instances where analytical instruments have control systems that are not networked into an overall Lab system and operate as Stand Alone systems. Common examples are FTIR instruments, spectrophotometer instruments, etc. • Verify that Data Integrity control strategies have been implemented for these systems • Verify these strategies sufficient to prevent data loss or provide a warning of potential DI issues		

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
	Printouts from these instruments are sometimes provided as “raw data;” however, paper printouts do not meet Data Integrity requirements because they are not the original raw data. Scan data is captured digitally and is, therefore, dynamic in nature and susceptible to changes. In addition, paper printouts cannot capture the metadata from the associated file. When the primary records are printouts from these systems, request a review of documents from various instruments, i.e., an FTIR and a spectrophotometer. • Determine if the associated data is static or dynamic in nature • Determine when and how the relevant data was relegated to a static record • Verify that the record is Date and Time stamped, with the individual identified that performed the analysis • Determine if “metadata” added/written to the printout is sufficient to allow a full history of the activities completed		

Data Integrity Auditing Checklist / Guide			
Laboratory Systems			
	Another concern with Stand Alone instruments is the limited data storage capability generally found with these systems. • Verify that complete data records are routinely transferred to more permanent storage to prevent loss of data files • The completed transfer of data record must include the deletion of files on the instrument to prevent any further changes to files after data has been backed up		
	There may also be instances of less sophisticated stand-alone instruments such as Balances and Karl Fisher Titrators. Such instruments generally include a printer to capture relevant data. • Ensure that the instrument time and date settings are aligned with local operations, and cannot be adjusted by Analysts • If the instrument does not provide a printout with date and time, ensure that the Analyst adds their name, date, and time to the printout when the activity is completed • Ensure that the paper and inks used are not photosensitive or prone to deterioration; data records must be permanent and legible during the full retention period of the associated record		

Data Integrity Auditing Checklist / Guide			
Quality Culture			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
Elements to consider for DI Quality Culture	• Control the issuance of blank paper templates for data recording and reconcile at conclusion of activity. • Ensure controlled forms for recording GxP data are located where activity is taking place; limit need for ah-hoc recording and transcription.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 4. Principles	
	• Restrict the ability to change clocks used to record timed events.		
	• Restrict user rights to automated systems; specifically, to prevent data changes and ensure audit trails are turned on and cannot be turned off by users.		
	• Ensure proximity of printers to sites of relevant activities, and ensure that automated data capture (printers) are connected to equipment, i.e., balances, pH meters. • Ensure controls are in place to ensure records recorded via temperature-sensitive or photosensitive inks/paper (e.g., thermal paper) are not subject to data loss.		
	• Ensure access to original data records for staff performing data review activities.		

Data Integrity Auditing Checklist / Guide			
Quality Culture			
Established process for Quality Manager to communicate DI metrics to Senior Management.	• Tracking and trending of invalid or incorrect data. • Results of audit trail reviews, specifically those reviewed as part of a key decision-making step. • Results of routine audits and self-inspections of computerized systems. • Monitoring of contracted or outsourced entities; tracking and trending of associated quality metrics for these sites.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 6. Governance and Quality Audits	
System Administration of computerized systems should be allocated to independent IT support personnel, to manage system security, data backup and archival, etc.	• FDA guidance recommends maintaining a list of all authorized individuals and their access privileges for each cGMP computer system in use. • MHRA Guidance allows for “limited” use of controls established by dual user accounts with different privileges for organizational structures with limited resources. In such cases, all changes to data must be independently reviewed and approved.		
Ensure roles and responsibilities for assurance of complete and accurate data and records are established and robustly maintained for outsourced providers.	• Documented process for both parties are developed to ensure data integrity. • These processes, and expected data integrity control strategies, should be clearly detailed in the contract between the organizations.	WHO Technical Report Series No. 996, 2016, Annex 5 - Section 7. Contracted Organizations, Suppliers, and Service Provider	

Data Integrity Auditing Checklist / Guide			
Quality Culture			
Particular focus should be given to outsourced database and software providers, including cloud-based service providers.	• Service providers must ensure that personnel are appropriately qualified and trained in Data Integrity controls and practices. • Service provider's activities must be monitored on a regular basis (via routine audits), at intervals determined through a risk assessment of the data and record criticality.		
Assess oversight of subcontractors and suppliers for Outsourced Providers.	• Audit outsourced provider to determine internal controls over suppliers and subcontractors; select examples to assess from formal listing of authorized subcontractors working for the outsourced provider. • DI control strategies should be included in quality agreements, contracts, and/or technical documents. • Outsourced provider should have access to supplier's or subcontractor's relevant data and electronic records, including audit trails, reports, and other paper or electronic records.		
Established data control strategies for contracted data backup and record archival activities.	• Should include documented processes for data ownership and data retrieval from third party service provider. • Documented agreements should provide provisions for access and transfer of data and records in the event of the third party service provider closure, etc.		

Data Integrity Auditing Checklist / Guide			
Quality Culture			
Audit Trail Reviews	Changes to critical data should be reviewed with each record before final approval. Items reviewed would include change history of finished product test results; changes to sample run sequences; changes to sample identification; changes to critical process parameters.	FDA Guidance for Industry – Data Integrity and Compliance With cGMP – DRAFT – April 2016	
Personnel responsible for Audit Trail Reviews	Personnel responsible for record review under cGMP should review audit trails that capture changes to critical data. For example; production control records, and audit trails, must be reviewed and approved by the Quality Unit.		
Acceptability of paper printouts.	If data is a static record, i.e., printout from pH meter or balance, this may be acceptable. Most other data from lab instruments are dynamic, i.e., may be reprocessed, which is not acceptable as complete record.		
	Original laboratory records must be subject to second person review to ensure all test results are appropriately reported.		
Reprocessing of chromatography records.	Must have approved procedures to follow for reprocessing; all reprocessed results must be retained; complete records would include raw data, graphs, charts, and spectra from Lab instruments.		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
ERP Systems	Enterprise Resource Planning (ERP) systems generally provide oversight of manufacturing needs, to include procurement activities, testing and release of incoming supplies, batch record controls, materials management, and final product review and approval for market distribution.		
	The same system configurations, as noted for other systems, will need to be implemented: • Unique user accounts, with individual passwords; routine revision of passwords • User account system authorities and functions allowed for each authority • Audit Trails are on and cannot be turned off • System Date and Time clock aligns with local operations • System data records and files must be subject to routine backup and archive operations		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
	Verify system functions for oversight of procurement activities and materials management: • Materials are procured from only approved suppliers • Determine system functions for receipt (including unique tracking numbers), sampling, testing and approval of incoming materials • Evaluate how material status is controlled throughout the entire manufacturing sequence, including material on hold (not yet released, or under investigation) or rejected (not meeting requirements) • Review the process for generating a manufacturing "ticket", with particular attention to the structure of the Bill of Materials (BOM) • Determine how system is updated as materials are consumed in the manufacturing process		
	The following items should be verified: • When approval of the final product is conducted in the ERP system, verify that the Quality Unit provides the final review and approval of finished product lots for market distribution • If approval occurs in LIMS, then an appropriate material status update must be provided to the ERP system		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
	The overall objective is the ability to recreate the sequence of events during the manufacture, approval, and distribution of finished product. Ensure that the data records and files include the appropriate date and time stamps, and the identification of the user completing the various functions.		
Warehouse Management Systems (WMS)	There may be instances where the materials receipt and storage functions are conducted by a warehouse management system outside of an ERP system. The following DI items should be evaluated during an audit: • Materials are received against a purchase order from an approved supplier • Each individual receipt of material is assigned a unique tracking number (Lot Number)		
	Conduct a walkthrough of the warehouse facilities, evaluating the following items: • Warehouse system is capable of providing storage/rack location, quantity, and current status for each material Lot (usually through a bar code function) • Verify correct data is pulled from the WMS, specifically looking at quarantined or rejected material lots • The WMS has a validated interface with the ERP or manufacturing planning system and provides immediate updates as the material moves from receipt through production processes		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
Building Automation Systems (BAS); monitoring and alarm for environmental conditions	The primary function of these systems is the monitoring, recording, and control of room temperature and/or humidity conditions. The scope of such “systems” range from simple chart recorders, to highly sophisticated networked systems of monitors and recording devices. The validated monitoring and recording of BAS data (environmental conditions) is highly significant with respect to classified rooms/space, i.e., Sterile Operations areas.		
	The initial inquiry for such systems should be a completed mapping study of the space being evaluated. • The primary focus of mapping studies is to determine the “worst-case” locations of monitoring probes within the room environment, i.e. worst-case locations for high bay warehouses are generally in the upper storage racks. • For regions with significant seasonal variations, a warm weather study and a cold weather study should be completed.		

	The following items should be verified when evaluating a mapping study: • Mapping study conducted via formally approved protocol. • Protocol details number and location of study probes, and time period for collecting study data. • Study probes have been calibrated pre- and post-study period. • Evaluate study conclusions; number and location (if study probes are sufficient); data is complete from each probe for the date and time duration detailed by the protocol; data analysis has determined worst case locations for monitoring and control of the area studied. • Verify operational probes have been placed at worst case locations and data collection is appropriate (i.e., continuous vs. periodic logging of data) for each area.		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
	Evaluate data management practices for environmental monitoring: • Chart recorders have the name, date, and time the chart was set up; and the name, date, and time the chart was removed from the recorder. • Log in to BAS program must include the use of unique user accounts and passwords. • An audit trail must be in place to provide the name, date, and time stamp for any activity completed on the system. • Data records must include the location, date, and time data was recorded. • Data analysis, and subsequent reports, should be validated.		
Automated Production Equipment (Networked or Stand Alone)	Most production equipment is operated through a human-machine interface provided by an automated controller. Equipment can operate as a stand-alone system, with functions being directed by the controller, or networked into a highly sophisticated Distributed Control System (DCS) providing operational control of an entire manufacturing process. A DCS will generally provide operational control of the manufacturing process according to an approved Batch Record, collecting specified manufacturing data, and generating a completed batch record at the end of processing.		

Data Integrity Auditing Checklist / Guide			
Manufacturing Control Systems			
	Evaluate a system for the following: • The use of unique user accounts and passwords. • Audit Trail is functional and cannot be turned off by the user; Audit Trail identifies the user, date/time stamp, and function being performed by the user. • System should be configured to provide sequence control of the manufacturing process. • System should be configured to require signature and date/time stamp for each identified “critical” process step (i.e., material charging is generally a critical step and would need to be initialed and date/time stamped before proceeding to charging the next material). • Process data must be backed up in a sufficient manner and time period to ensure that data will not be lost. This is particularly important for stand-alone controllers that may have limited storage space for data recording.		

Data Integrity Auditing Checklist / Guide			
Enterprise & Quality Systems			
Audit Subject	**Description / Inquiries**	**Regulatory Reference**	**Auditor Observations / Comments**
Training Management Systems	Training systems are utilized to provide documented evidence that employees have been properly trained for their job function within the organization. • Job descriptions detailing each position's functions and training requirements.		
	Data integrity areas of interest are as follows: • System is configured for unique user accounts and passwords. User accounts include system authorities and restrictions for each user. • Audit trail is functional and cannot be turned off by the user. • Training data includes the individual completing the training assignment, date and time training was completed, and training module name. If the training module was an instructor-led session, the records should also include the Trainer identity and time duration of the class. • Data analysis and subsequent reports are validated. • Personnel whose job functions are impacted by implemented changes should be informed and assigned additional training modules as required.		
Document Management Systems	The generation and revision of documentation and records must be managed under a structured process.		

Data Integrity Auditing Checklist / Guide			
Enterprise & Quality Systems			
	Data integrity needs include the following: • Access to documents for revision and/or generation must be restricted to appropriate individuals, i.e. Author, Reviewer, Approvers. • Documents, and formal procedures, must be readily available to organization personnel, at their respective work spaces. • Distribution or availability of revised documents must be controlled to ensure that previous versions are not being used by personnel. • Outdated versions should be archived for a determined retention period.		
Data Storage Systems	Data storage systems are intended to prevent the loss of data and allow for the re-creation of events, manufacturing process activity, etc., at a future time or inquiry.		
	Data and record storage systems must be subject to routine backup activity to ensure that any data loss can be recovered in a timely manner.		
	Backup functions may include a variety of backup plans to cover high risk contingencies, i.e., daily changes to data, weekly backup to on-site storage location, and monthly full backup to an off-site location.		
	Data backups are performed to allow recovery of dynamic data, so the backup must also include metadata, including audit trail records.		

Data Integrity Auditing Checklist / Guide			
Enterprise & Quality Systems			
	Data should be archived periodically in accordance with written procedures. • Archive copies should be physically secured in a separate and remote location from where back up data are stored. • The data should be accessible and readable and its integrity maintained (including metadata) for the entire period of archiving (record retention period). • There must be a procedure in place for restoring archived data in the event of an investigation. This procedure should be regularly tested.		
	Storage media must be evaluated to ensure that the media is not eroding over a period of time. Tape and disk storage systems can erode and will need to have appropriate refresh periods established to cover any retention periods required.		