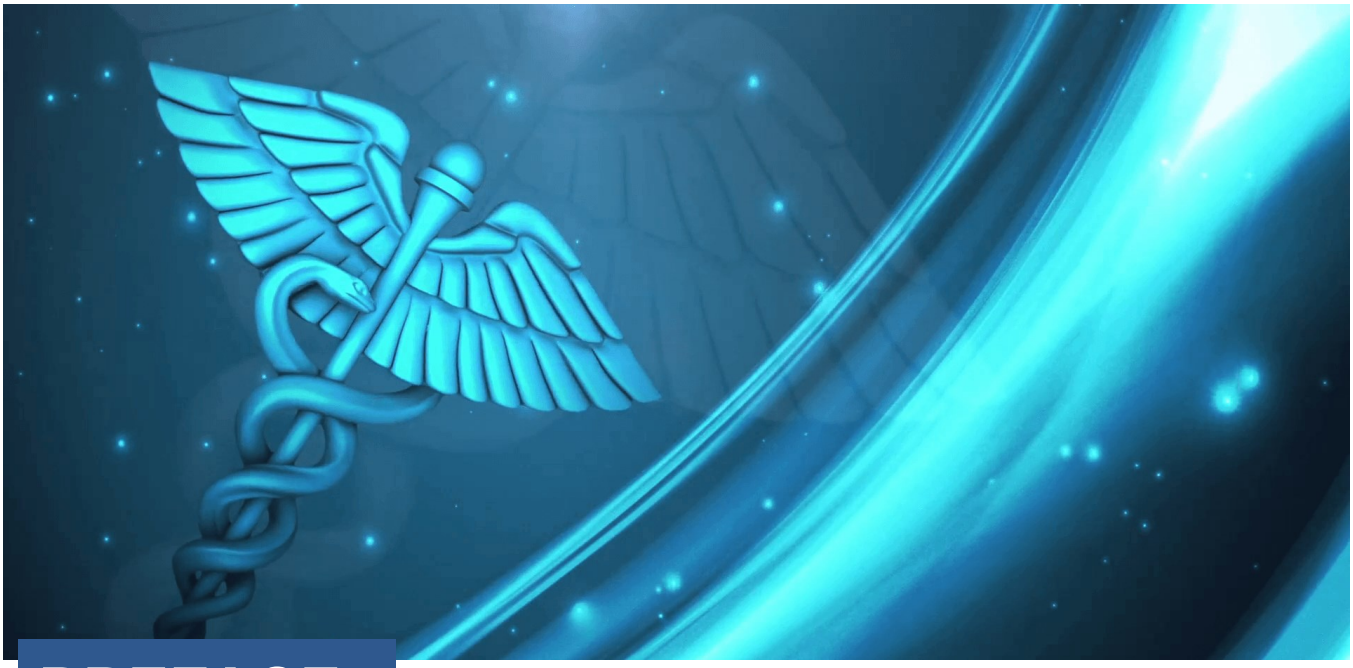
Best Practices on Digital Data Management 21 CFR Part 11 Compliance

Guidance on Digital Data Management

21 CFR Part 11 Compliance

CONTENTS



PREFACE

In April 2015, The IPA launched its Quality Forum (QF) to help Indian pharmaceutical manufacturers to achieve parity with global benchmarks in quality. The QF made a commitment to a multi-year journey to address key issues facing the industry and develop best practices.

The QF focused on several priority areas in the last four years, namely, Data Reliability, Best Practices & Metrics, Culture & Capability, Investigations, etc. It took upon itself the challenge of developing a comprehensive set of Best Practices Documents for several of these topics. In this document, we focus on best practices for Digital Data Management – 21 CFR Part 11 Compliance. We had released a comprehensive set of Data Reliability Guideline in February 2017, Process Validation Guideline and Good Documentation Practice Guideline in February 2018, Investigation of non-conformities in February 2019 and Handling Market Complaints Best Practices in February 2020.

The six participating companies in the QF nominated senior managers to study the best practices and frame the guidelines. They are: Ramakant Shukla (Cipla); Rajesh Thempadiyil (Dr Reddy's); Rajeev Bedage (Lupin); Aparna Mazumdar (Sun); Pranav Dalal (Torrent) and M Ravisankar (Zydus Lifesciences). The IPA wishes to acknowledge their concerted effort over the last 12 months. They shared current practices, benchmarked these with the existing regulatory guidance from the USFDA and other regulatory bodies such as UKMHRA, WHO, etc., developed a robust draft document and got it vetted by a leading subject matter expert and regulatory agencies. The IPA acknowledges their hard work and commitment to quality.

The IPA also wishes to acknowledge the CEOs of six member-companies who have committed their personal time, human resources and provided funding for this initiative.

This document, to be released at the IPA's Advanced GMP Workshop 2022, will be hosted on the IPA website www.ipa-india.org to make it accessible to all manufacturers in India and abroad.

MUMBAI
OCTOBER 2022

1 Introduction

Regulatory guidance and adherence to follow those requirements in routine GMP activities is key factor for GMP compliance in pharmaceutical industry. In last decade many manual processes have been digitally transformed to most sophisticated and automated practices which helped to streamline and strengthen the manufacturing operations along with associated activities and to improve resource utilisation, compliance, and productivity in large extent in entire pharmaceutical end to end supply chain system. Also, there are many systems implemented & adopted in different domains of pharmaceutical industry like, manufacturing, quality, distribution, which are managed and used with all possible required mandatory standards and controls as per regulatory guidance. In this document, we have addressed few areas around data life cycle and widely adopted recommendation across pharmaceutical industry associated with different GxP systems.

2 Digital Data and Content Management

- In Digital world, data is important asset to any organization. Data can be used to make informed decisions and can apply different type of analytics like Descriptive, Predictive and Prescriptive to get the best results from the data. Organization should ensure that they are maintaining data quality during entire data life cycle.

- Organisation should establish the robust framework for Data Lifecycle Management and Data Governance to ensure the standard procedures & practices are followed across the organization. The data life cycle consists of different phases from data generation, processing, review and reporting, retention, and retrieval, to destruction. System design and controls should ensure appropriate detection of errors, omissions, and aberrant results throughout the data life cycle. Data Integrity controls should ensure ALCOA+ principles like Attributable, Legible, Contemporaneous, Original, accurate, complete, consistent, enduring and available.

- The regulated company should ensure the appropriate risks are identified associated with business processes to understand the data flow between different processes, systems, regulatory agencies and external organizations etc.

2.1 Data Generation

- Data can be generated by manual entry into a computerized system, or data can be acquired/collected from the instrument/equipment. Preferably data capture should happen without manual interruption to avoid the transcription errors. Computerized system should ensure the data captured is readable and should capture the details of the source of data and details of the data creation/modification, action performed by, date and time stamps etc. Time and date changes should not be permitted in the computerized systems to avoid the unauthorized changes to the data and system. Computerized system should ensure meta data of the data is captured and available in the system.

- Data generation & storage should happen contemporaneously during the execution of operation/activity. All the created data should be retained and should be available for review. System should capture the audit trail of all the events and data modifications. So that trail of events can be restructured in case of any requirement.

- Systems with limitation in the storage, organizations should explore the solutions to connect with the data capturing systems. i.e Connecting the manufacturing equipment to Data Acquisition Systems (DAS) or connecting the balances/pH meters to laboratory information management system (LIMS) etc.. If no possibility, paper records should be maintained.

- Testing of data integrity controls and data transfer between the systems should be verified during the qualification.

2.2 Data Processing

- Created/stored data is processed to interpret and generate the information in required format. Data processing can be performed using the defined process or methods as per the approved procedures. Standard Operating Procedures should encourage the auto processing methodology based on pre-defined processing parameters, so that they can eliminate manual intervention. During the data processing, system should capture the name of the person who has processed/re-processed the data, processing date and time in the audit trail.

- Regulated company should establish standard procedure for reprocessing of any type of data and it should be oversighted by quality unit. All the test results should be retained for review, including all data related to iterative processing runs. Data re-processing impact will vary for the product/process; hence the organization should ensure that the robust risk assessment process to address the different risk scenarios.

2.3 Data Review and Reporting:

- This phase will cover the data review, reporting and use of the data. Data review process should consider the pre-defined acceptance criteria defined in the approved procedures and regulatory requirements. Prior to performing the review, reviewer should have understanding on the process/system, impact on patient safety and product quality, system generated data and data review requirements. The data review process and frequency should be documented in the standard operating procedures. Outcome of all the data review and conclusion should be documented.

- Regulated companies should establish the procedure for the data and audit trail review. The procedure should define the check points to be verified and type of verification (Batch/Periodic) and handling of the discrepancy observed during review. Data and audit trail review procedure should cover the definition of software error codes and critical alarms for the uniform interpretation within different type/role of users. During the review process, reviewer should conduct the review based on the original data, relevant meta data, and audit trail of the data. Audit trails should be reviewed for the critical changes/events/actions, which are associated with data and systems.

2.4 Data Retention and Retrieval

- The data should be stored in secure location that has adequate physical and logical controls throughout the retention period. Original Data or archived data or backup data should be retained securely as per the applicable regulatory requirements and organization policies during operation phase of system or after system retirement. Retention period for different types of data should be assessed, determined, and documented in procedures. Data should be readily available through the defined retention period as per the approved procedures of organization.

- The organization should maintain the procedures for the access management of the servers (Physical and Logical), data backup and restoration, disaster recovery procedure. Data should be stored in different geographical location to safeguard the data in case of any natural disasters or cyber incidents. The procedure should cover about disaster recovery process and testing of recovery. During initial testing, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and periodic testing should be performed.

2.5 Data Destruction

- Data destruction should be handled with appropriate practices in line with quality management system. Data destruction should not impact the good operational data and critical data. Organisation should have the procedure for the data destruction handling, and it should cover procedure for the identification of data to be destroyed/disposed, conditions of disposal and access management of the data disposal, controls for verification of destruction data and discrepancy handling. The procedure also should cover local laws, regulations, and best practices on electronic waste management.

2.6 Data Integrity Risk Assessment (DIRA)

- The regulated company should ensure the robust Data Integrity Risk Assessment (DIRA) process is in place to handle the potential risks and mitigations throughout the data lifecycle. The DIRA should cover all the risks associated with the system data life cycle includes data generation, data transfer, data modification, data availability and data destruction etc. While performing the risk assessment for any computerized system, organization should assess the possibilities of data integrity breaches and should implement appropriate mitigation actions. During the risk assessment, organisation should consider compatibility of the different systems, data formats, interface systems (if any), data generation rate vs data transfer rate and communication failure scenarios etc. Organisation should ensure the controls and mitigations are implemented based on the risk assessment for the data transfer between the systems.

- The methodology of risk assessment for the Data Integrity consists of the activities such as identification of risks in the functions, deciding on the mitigation actions for each of the risk, executing them, tracing, and determining the residual risks. Below are the identified potential risks in the view of Data Integrity throughout the Data lifecycle, based on the appropriate level of controls required, organisation can define the mitigation plans.

Table-1: Key Potential Risk Areas

Sr. No.	Section	Potential Risk Areas
1	Security and Access Management	Inadequate Physical security controls w.r.t. Servers and clients
2		Lack of access authorization and management
3		No Unique user identification
4		Lack of pre-defined role-based or privilege-based user authorization
5		Unrestricted access for write, update and delete
6		Inappropriate Password Policies i.e no password changing, no password complexity, no Idle time logout
7		Sharing of user credential
8		No automated measures on attempted unauthorized access (e.g., lock account, notify management)
9		Ineffective Periodic access rights review
10	Backup and Restoration	Inadequate procedure for backup and restoration
11		Outdated Backup methodology
12		Failure of Backup execution and monitoring
13		Inadequate investigation of backup failures.
14		Inadequate media management (e.g., labelling, storage, rotation, refresh)
15		Lack of high availability system architecture
16		Manual backup execution
17		Challenges leading to failure periodic restore verification
18	Disaster Recovery and Business Continuity	Lack of Service level agreements
19		Lack of defined and tested procedures disaster recovery.
20		Lack of defined business continuity plan.

Sr. No.	Section	Potential Risk Areas
21	Audit Trail	Lack Procedure for clarity interpretation of the audit trail data.
22		Lack of appropriate controls for security of audit trails.
23		Missing events or actions in the audit trail.
24		Lack of control on Date and Time change settings
25		No Backup and Restoration of the audit trail
26	Software Controls	Missing functional controls
27		No User identity checks
28		Automatic functionality to reduce human error
29		Failure to store the data during acquisition
30		System rebuilds or Patch implementation
31		No Sequence enforcement for serial actions
32		Lack of data entry validation
33		Lack of Error or Alarm handling
34		Lack Prompt for confirmation of action
35		Monitoring tools (e.g., event logs)
36	Hardware Controls	Lack of Mirrored or RAID drives
37		Lack of Mirrored or RAID drives
38		Lack of UPS connection
39	Policies and Procedures	Lack of Mirrored or RAID drives
40		Lack of System Administration and Security Procedures
41		Ineffective procedures and working documents
42		Inactive engagement of the stakeholders
43	Training and Experience	Inappropriate review and approval GxP data/activities
44		Ineffective training of all the stakeholders
45	General Points	Inadequate Change and Incident Management practices
46		Unavailability of system at locations where activities take place
47		Inadequate verification of Interface with other systems
48	Interface with other systems	Incorrect usage decision status posting from one system to other system.

3 Walk through for GxP requirement for electronic/digital data handling.

GxP computerized systems in pharmaceutical industry has critical impact on each of GMP activities performed and managed using these systems. As per regulatory guidance's each GMP system need to fulfil different regulations published by USFDA, EU, MHRA regulations etc so that product quality, patient safety and data integrity aspects to compliance for each product to be manufactured and distributed to patient. Below are the regulatory requirements for electronic data and security controls mentioned along with its high-level impact areas and industry best recommendations to meet requirement and eliminate potential risk & impact on patient safety.

Table-2: Walk through and recommendation for GxP requirement

Sr. No.	Item	Potential Risk/Impact	Recommendations
1	Systems should create and capture, correct & accurate data	Invalid data or wrong data entry	System should be configured/designed/validated to create & capture the accurate data in correct and valid format. • Wherever possible capture data from source system through interfaces. • Critical Data fields should be configured as mandatory field with data validation for interface & manual entry. • Wherever appropriate, interlocks should be configured for any exception handling. • Raw data should be saved such that it is not vulnerable to manipulation, loss or change.
2	Verification of manual entries of critical data	Data may be wrong/not appropriate	Data should be verified either by a second person, or by computerized system itself e.g., data validation through range.
3	Any changes to data should be authorized and controlled.	Manipulation of data e.g Reprocessing of laboratory results.	Any changes and modifications to raw data should be fully documented and should be reviewed and approved by Quality team.
4	User access controls should be configured, granted, and enforced in routine operation.	Vulnerable to data integrity breaches.	Manual or automated systems for granting access should be implemented to ensure physical and logical security, and to prohibit unauthorized access to, changes to system and deletion of data.

Sr. No.	Item	Potential Risk/Impact	Recommendations
5	Any request for new users, new privileges should be authorized by appropriate personnel.	Traceability for user creation and privilege modification is not maintained.	Procedure should be in place for user creation and maintenance in GxP system. Reconciliation for user creation or modification or deactivation should be performed on periodic basis.
6	Systems must support Individual Login IDs with pre-defined role-based privileges	Generic login credentials will not have traceability for actions performed	Software should be implemented with individual login ids & role-based privilege configuration. In Legacy systems equivalent control shall be provided • by add-on third party software, or • by paper-based manual method (capturing who, when, what, why, action performed, reason and 2nd person check) to ensure detailed traceability • Reconciliation and rigorous periodic review for use of such credentials against system, batches, process, documentation etc. • In-worst case, we can use external video recording tools to ensure authentic event log.
7	Deactivation of inactive users	Sharing of retired/dormant user credentials to perform unauthorized actions.	Automated tools should be implemented to integrate various different systems so that to adopt “Disable one and Deactivate all” i.e. Active Directory integration. Alternatively, process shall be in place to ensure deactivation in every system before person leaves the organization or on periodic basis.
8	User ID and passwords should be periodically checked and revised.	To maintain Password confidentiality	System should be configured to prompt for revision of password after pre-defined intervals.
9	System administrators should be independent from users	Inadvertent changes to validated system by user.	Dedicated technical team should be identified and assigned administration tasks, who should not have interest on data in the system.
10	Computerized systems should have provision for an auto-lock/logout.	Unauthorized access of system/data and modification.	Auto-lock or Auto-logout should be configured in system either at the application or operating system level. Procedural control should be in place where system does not support auto-lock/ auto-logout so that user manually logout..
11	User access for local drive and operating system should be restricted.	Control panel access may lead to change validated state, in data, and system performance parameters	Procedure should be in place to restrict user access for • Control panel -Cut/copy/delete/right clicks. • Local drives/programs. • Windows auto-update
12	Computerized systems & data should be protected.	Accidental changes or deliberate manipulation	Computerized system should be restricted for • Any type of auto-updates like windows, antivirus, application etc. • Date/time access to authorized personnel • Hardware and software should be appropriately secured and restricted to authorized personnel.

Sr. No.	Item	Potential Risk/Impact	Recommendations
13	Restrictions on external USB drives and devices	Information Security threat due to use of USB devices	Procedural and technical controls should be in place to restrict the use of such devices Restricted usage of external USB drives & devices.
14	Built-in checks for the correct and secure exchange of electronic data.	Inappropriate data exchange and data alteration.	It should be ensured that validation has been performed to checks that data is correctly exchanged and not altered in value or meaning during this migration process with appropriate Data Integrity controls.
15	In case of software upgradation, it should be ensured that new version/application can read existing and archived data	Existing Data availability and readability in case of software upgrade	Existing data readability in new version/ application should be validated during data migration process. In case, existing data is not readable in new software, the old software should be maintained as per approved procedure and should be reviewed periodically.
16	Data backup & restoration verification.	Incomplete data backup and Data loss. Backed up data is not readable and accurate at the time of restoration.	Data backup and restoration frequency should be identified considering system complexity, data type and eliminate redundant efforts in case of periodic restoration verification Automated tools should be implemented for system driven data backup and verification. Backup records should be periodically reviewed and approved by Quality team. Manual data backup activities in legacy systems should be witnessed by 2nd person preferably Quality team representative during it is being performed.
17	Electronic data & Printout	Poor controls to maintain integrity of electronic data Redundant efforts for printing	Electronic data need not be printed in Paperless environment where significant data protections controls are implemented, and data/system is safeguarded for entire data life cycle and retention period. In case required, it should be possible to obtain clear printed copy of electronically stored e-records. For records supporting batch release, it should be possible to generate printout to indicate if any of the e-records has been changed since the original entry.
18	Audit Trail Records & significant of different actions in audit trail.	Intentional or accidental modification/deletion of records.	Audit trails record with every critical and significant action associated to validated state of system and data must be available, protected and regularly reviewed. Clear procedure should be established to evaluate which data and actions are critical/significant, to be recorded in audit trail.
19	Is electronic signature mandatory	Electronic Signature provision is not available in every software.	Electronic Signature is mandatory in case of paperless environment, and it is not mandatory in paper-based environment. Electronic signature along handwritten signature may be applied in case of hybrid environment

Sr. No.	Item	Potential Risk/Impact	Recommendations
20	Change management in validated systems	Changes implemented without appropriate assessment.	Any change to a validated computerised system should be appropriately evaluated before implementation to understand overall impact on data integrity and product quality. The evaluation should consist existing data on the system, product manufactured/analysed, data integrity controls and legacy documentation.
21	Incident and breakdown management	Uncontrolled and inadequate handling of issues.	All incidents associated with system malfunctioning, data errors, should be registered, investigated, and reconciled. Appropriate corrective and preventive action should be identified & implemented based on actual/most probable root cause and implement CAPA effectiveness should be verified periodically. Periodic trending and assessment for all incidents should be performed to understand system performance and improvement areas.
22	Periodic review and assessment of System & Data	Compromise in validated state of system and data integrity controls.	Periodic review of validated computerised system should be performed considering routine operational use, validated range of functionality, change records deviation records, incident, upgrade history, system performance, System reliability and security, validation status.
23	Data Archival	Archived data is not readable.	Data can be archived based on requirement to improve system performance and to safeguard the existing data. Archived data should be verified periodically for the accessibility, readability, and integrity.
24	Data Destruction	Manageability of data and impact on system performance.	Appropriate procedure should be established to evaluate retention and destruction strategy of any data generated in GMP environment. Data should be destroyed as per data retention/destruction policy.
25	Data Life Cycle Risk Management	Potential risks of at different stages of data life cycle.	Procedure should be established for the Data life Cycle risk management to evaluate potential risk during data creation through data destruction. Risk management should be applied throughout the lifecycle of the Data/computerised system considering patient safety, data integrity and product quality.
26	Cyber security initiatives for data & system security.	Cyber security threats to sensitive and critical data/systems	Robust information security practices should be implemented • Information Security Policy, • User awareness for different threats • Periodic review mechanism should be in place to detect potential security threats and initiate proactive measures to restrict. Proactive assessment and monitoring of vulnerabilities

4 Challenges for Legacy systems and other areas

Each organisation will always have some legacy systems which are used in routine operations and business requirement. Legacy system which may not have all the required technological enhancements to handle business and operational challenges which need add-on tools or procedures to manage and help organisation to continue using these systems. Below table has few examples recorded capturing challenges and tentative recommendations to handle such challenges. Recommendations should be evaluated appropriately before implementing in each organisation ensuring product quality, patient safety and data integrity aspects. The legacy systems, that are recording/generating the Critical Process Parameters (CPP) or Critical Quality Attributes (CQA) or any parameter value into GxP Records should be prioritised to enable required controls. If the legacy equipment (i.e., Induction Sealer, bottle un scrambler etc..), do not generate any parameter value, decision should be taken based on the risk.

Table-3: Industry challenges and recommendation for GxP systems.

Sr. No.	Challenges	Recommendations
1	**HMI Based systems** • Limited/No data storage, no audit trail, limited/no data integrity controls, • Limited capabilities as per 21 CFR Part 11 requirement. • System access & operation using common User credentials. • Time synchronisation issues • No capability for printout.	• Implementation and integration to Centralised Data Acquisition System • Upgradation of HMIs with data storage & protection capabilities. • Short Term- Manual logbook to record each activity performed with activity name, user details, start/end date time, changes etc & second person witness. • Maintain list of users accessing such systems with periodic review. • Procedural controls should be ensured for routine review of time and rectification. • Long Term- Replacement of HMI with data storage & Data Protection capabilities. • Conversion of data into electronic form like PDF etc. and retain as required. Image capture wherever feasible and convert into electronic form
2	**OEM support** • Delayed/no response for vendor/supplier assessment • Inherent discrepancies in newly procured system • Capability and lead time towards technical resolutions. • Clear & complete documentation in case of breakdown & issue resolution, new version releases	• Identify alternate vendor with faster resolution and complying internal standard. Vendor Acceptance based on risk assessment for impact on product & system during routine operation after implementation. • Wherever possible, establish internal skillset and capabilities to address technical challenges to reduce and eliminate business/compliance impact. • Define and agree clear expectation during initiate procurement to handle breakdown & issues.
3	**Breakdown & Like-to-Like Replacement.** • Equipment breakdowns and hardware replacement. • Equipment breakdowns and software reinstallation.	• Risk based approach to evaluate and implement equivalency for old and new component if it is same make/model/configuration. Equivalency study should help to implement Like-to-Like replacement methodology with reduced efforts achieving business and compliance. • Adopt Image backup technology to address reinstallation of qualified image for breakdown rectification with appropriate change management approach.

Sr. No.	Challenges	Recommendations
4	**Time Synchronisation mismatches.** Time mismatches in instrument & equipment	Routine monitoring of date/time through procedure. Windows Time services in background processing should be correctly configured and working, so that accurate date/time is fetched from domain servers. Periodic monitoring of domain/time server performance i.e., Network Time protocol configuration and health check. Domain Server is a best option for time synchronization as it can be managed centrally without manual intervention and probabilities of time mismatch are very less for network connected systems. Workstation hardware/bios time configuration should be disabled. Scheduled replacement and verification of CMOS battery wherever applicable. Appropriate Time Zone Settings are maintained during initial implementation to ensure date and time are synchronised with respective geography with correct time of that location. Daylight time settings should be verified if it is configured in system by OEM. Use of third-party software tools which are installed on the client to synchronize the time of systems which are connected to network. Manual time synchronization method required where systems are not connected with Network, it is manual activity where time of each system needs to be adjusted manually with reference to master clock on stringent frequency like daily basis. Proactive monitoring of different components like CMOS batteries, NTP settings, Windows times services etc. Routine rebooting of key servers/clients etc for better performance.
5	Health check of legacy (retired) systems and data stored in such systems	Retired Legacy systems should be retained only in case there is dependency of system/application to read/restore the data for future reference. Retired Legacy system should be retained for definite period based on critically of system & data, operatability of instrument and application, vendor/OEM support. Many retired systems may not work as intended due to wear and tear of electronic components and known life of the components. Hence, such retired legacy system should be verified on routine frequency for data readability and to check application/system condition.
6	Huge data generated in Audit trail of manufacturing systems which is herculean task to review and interpret and may not be able to provide significance.	Regulated companies should have written procedure in place to review batch report, recipe report, alarm and event log based on critical risk areas identified with the help of OEM. Also, system administration procedures should be enforced to review and ensure all the system configuration changes and user administration activities are reviewed and documented. Usually, every manufacturing system records many events as part of audit trail and each event may not have impact on product quality and data integrity. Hence critical identified risk areas should be reviewed as part of audit trail review. Any change in existing validated system should be handled through appropriate change management process.
7	Security patch updates in GMP Equipment & Challenges in operating the equipment i.e system crash, stoppages of system services and hence data loss.	Segregation of IT/OT setup. Test bed for testing of patch updates Engagement (i.e AMC) with OEM for pro-active assessment of impact of patches on equipment operation.

Sr. No.	Challenges	Recommendations
8	Human dependency for Data Backup in standalone systems using USB Drive/Hard Drive	Procedure with mandatory check points for execution and second person witness during execution. Connect with network and enable tool-based backup.
9	Restoration of backup data for standalone systems with database, availability of restoration environment (i.e Application, Licence, Hardware) and impact on existing operational system.	Matrixing and bracketing approach; based on type of system/equipment/ application/database. Perform restoration for selected systems based on the approach & risk assessment.
10	Modification or deletion of Raw data files from operating system.	Critical controls should be implemented for windows workstation level or domain group policy to ensure appropriate data integrity and compliance. Below are few controls: Disable access to Date/Time & Time Zone modification, Disable task manager Disable right click Disable 'Run, Search, personalised menu Disable Network connection' from Start Menu System inactivity locking in minimum time Prevent access to the command prompt Disable Recycle Bin and Network shared Drive Restrict registry editing tools and Turn off Auto play Restrict control panel access, External Drive access (USB, CD/DVD/HDD, Memory card, tapes etc.) Disable internet except Business URLs.

5 Cloud based systems implementation and handling.

Every organisation is looking at implementing cloud-based setup for GxP systems as a technology enhancement to achieve operational and compliance benefits. Cloud setup gives edge over faster IT infra readiness, improved performance, and globally uniform platforms.

Table-4: Potential impact areas and recommendation

Sr. No.	Item	Potential Risk/Impact	Recommendations
1	Cloud service provider qualification as part of supplier assessment	Risk in vendor maturity and reliability of product and support services	SOP should be in place to evaluate cloud service provider on key aspect like software development life cycle, quality management system, change management data integrity, data privacy and product maturity and vendor reliability, operational support. Assurance of Uninterrupted services during operational use of system, mainly for SaaS. Verify the certifications Systems and Organisation Control (SOC-2) and ISO 27001 or equivalent as part of vendor evaluation.
2	Compliance to regulatory requirement.	Regulated companies may not be able to validate complete system (e.g., IQ/OQ) to check all regulatory requirements due to cloud setup limitation.	Ensure that Cloud service provider has clear & appropriate validation policy and documentation in place. Leverage vendor validation documentation to evaluate adequacy to meet regulatory requirements and fitness for intended business purpose. Perform the risk assessment, identify the mitigations, and verify that the vendor document covers the mitigations, perform the testing for missing mitigation action items.

Sr. No.	Item	Potential Risk/Impact	Recommendations
3	Data security of cloud system	Regulated companies may not be to test backup & restoration, IT infrastructure and security to overall cloud setup.	Ensure that cloud system must have in-built redundancy for overall system as well data generated and stored on the system to avoid any kind of data loss risk as part of vendor evaluation. Ensure Service Level Agreements (SLA) and Non-Disclosure Agreements (NDA) should be signed by the both the parties. Ensure that these agreements cover data security, data and system availability, data privacy, backup & restoration and Disaster Recovery etc. Verify the vendor testing document of backup and restoration program which ensures data security. System Configuration administration access is restricted and not provided to any organisation or user.
4	Regular version and patch implementation to validated system.	Updates to system are not in control of the regulated organization	Regulated companies should establish procedure to define the impact-based qualification. Classify the patch updates/version upgrades into major, minor and no impact, define the qualification activities as defined below. • No Impact: Patch updates/version upgrades are not having any impact on the existing functionalities of the system. Perform the impact assessment and leverage the vendor documents (IQ&OQ), no testing is required from the regulated company. • Medium Impact: Patch updates/version upgrades which are introducing new configuration/introduction of new functionality and no impact on existing functionality of the system. Perform the impact assessment and leverage the vendor documents (IQ&OQ), PQ testing may be required from the regulated company. • Major Impact: Version upgrade which are enabling the major functionalities. Leverage the vendor documents (IQ&OQ) and required set of validation deliverables should be created by the regulated company based on impact assessment. Cloud service provider must have written procedure to assess each change to existing validated system before the change is implemented. Also, verify the change communication procedure is available with vendor during the vendor evaluation and all the key stake holders email ids are configured for the change update communication to customers
5	Retirement of system in-case of system discontinuation.	Data generated by regulated companies will be available with cloud service provider.	Appropriate change management should be followed to discontinue use of system, deactivation of users, procedures and archival of records, data migration and archival within regulated companies. Master services agreement /non-disclosure agreement should be documented and agreed by both parties to ensure data security after system retirement. Ensure that the all the agreements are cancelled.
6	Periodic Review of validated system.	Cloud service provider may not provide access to complete setup and data to perform periodic review	Perform risk based periodic review to understand vendor change management program along with configuration management. Verify the completeness and correctness of each change implemented over the period using historical data available in validated system which are applicable to respective regulated company.

6 References.

1. **21 CFR PART 11**

   Electronic records; Electronic signatures

2. **EU ANNEX 11**

   Computerised Systems

3. **PI 041-1**

   PICS-Good Practices for Data Management and Integrity in Regulated GMP/GDP environments

4. **MHRA, Rev-01**

   'GXP' Data Integrity Guidance and Definitions

5. **GAMP**

   Record & Data Integrity Guide

INNOVATION. QUALITY. GLOBAL REACH.

Published by:
Indian Pharmaceutical Alliance
A-205 Sangam 14B S V Road, Santacruz (W)
Mumbai 400 054, India
E-mail: sudarshan.jain@ipa-india.org

October 2022