2026 Volume: 01 Issue: 08 ISSN 1671-2838 Page No: 52-75

Review Article

Pharmaceutical Care and Research

https://pcrjournal.com

Volume: 01
Issue: 07

DATA INTEGRITY AND QUALITY RISK MANAGEMENT IN PHARMACEUTICAL QUALITY CONTROL LABORATORIES: A REGULATORY AND RISK-BASED REVIEW OF ALCOA+ PRINCIPLES AND DIGITAL COMPLIANCE CHALLENGES

Marina J. Sapali*[1], Job Motta Mlaki[1], Bhavik Jani[2], Kushal Parekh[2], Pratik Vediya[2], Udit Trivedi[2], Ravi Ajudia[3]

[1]Student, [2]Assistant Professor, [3]Associate Professor

School of Pharmacy, RK University, Rajkot, Gujarat, India.

Article Received: 23 September 2026

Article Revised: 13 October 2026

Published on: 2 November 2026

***Corresponding Author: Marina J. Sapali**

Student, School of Pharmacy, RK University, Rajkot, Gujarat, India.

DOI: https://doi-doi.org/101555/ijpcr.7033

ABSTRACT

Quality control (QC) laboratories generate the analytical evidence on which batch release, shelf-life assignment and regulatory submissions depend. Over the past decade, inspections by the US Food and Drug Administration (FDA), the UK Medicines and Healthcare products Regulatory Agency (MHRA), European authorities and the World Health Organization (WHO) have repeatedly reported laboratory data integrity failures, including unreported trial injections, unjustified manual re-integration, shared log-ins and deleted raw data. This narrative review examines how the ALCOA+ principles, quality risk management (QRM) and computerized system controls can be combined into a workable data integrity program for pharmaceutical QC laboratories. Guidance from the FDA, European Commission and European Medicines Agency, MHRA, WHO, the Pharmaceutical Inspection Co-operation Scheme (PIC/S) and India's Central Drugs Standard Control Organisation was examined together with ICH Q9(R1), ISPE GAMP 5 (second edition) and peer-reviewed literature published between 1997 and 2025. The documents agree that records must be attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and available across their lifecycle, and that metadata and audit trails form part of the record. Recurring failure modes fall into technical, procedural and behavioral categories. Failure mode and effects analysis provides a structured way to rank these risks, provided its scoring subjectivity is managed as ICH Q9(R1) now requires. Compliance with 21 CFR Part 11 and EU GMP Annex 11, increasingly approached through risk-based computer software assurance, addresses the technical layer, while lasting data integrity also depends on management behavior and an open quality culture. Emerging issues, including cloud

hosting, artificial intelligence and the 2025 draft revision of Annex 11, are discussed with their implications for QC practice.

KEYWORDS: data integrity; ALCOA+; quality risk management; ICH Q9(R1); failure mode and effects analysis; 21 CFR Part 11; EU GMP Annex 11; audit trail; computer software assurance; quality control laboratory.

Abbreviations

API, Active pharmaceutical ingredient; CDS, Chromatography data system; CDSCO, Central Drugs Standard Control Organisation; CGMP, Current good manufacturing practice; CSA, Computer software assurance; CSV, Computer system validation; EMA, European Medicines Agency; FDA, US Food and Drug Administration; FMEA, Failure mode and effects analysis; GAMP, Good automated manufacturing practice; GLP / GMP, Good laboratory / manufacturing practice; HPLC, High-performance liquid chromatography; ICH, International Council for Harmonisation; LIMS, Laboratory information management system; MHRA, Medicines and Healthcare products Regulatory Agency; OOS, Out of specification; PIC/S, Pharmaceutical Inspection Co-operation Scheme; QA / QC, Quality assurance / quality control; QRM, Quality risk management; RPN, Risk priority number; WHO, World Health Organization.

1. INTRODUCTION

1.1 Operational role and evolution of quality control laboratories

Quality control (QC) laboratories occupy a central position in pharmaceutical manufacturing. They decide whether starting materials, active pharmaceutical ingredients (APIs), excipients, packaging components and finished dosage forms conform to their specifications for identity, strength, purity and quality before release [1, 2]. Routine testing produces a large and varied body of analytical evidence: chromatographic peak areas and integration events, spectroscopic profiles, titration end-points, dissolution curves, microbiological counts and long-term stability results. Batch disposition, shelf-life assignment and regulatory submissions all rest on this evidence, so the completeness and truthfulness of QC records has a direct bearing on patient safety [2, 3].

Over the last three decades the QC laboratory has moved from bound notebooks, hand calculations and printed balance slips to networked instruments controlled by software. High-performance and ultra-performance liquid chromatography (HPLC/UPLC), gas chromatography (GC), Fourier-transform infrared (FTIR) spectroscopy and automated dissolution testers are now standard, and their output is usually acquired, processed and stored by a chromatography data system (CDS) or laboratory information management system (LIMS) [4, 5]. These systems have improved sensitivity, throughput and traceability. They have also created governance problems that audit practices designed for paper did not anticipate: a printed chromatogram can look perfectly ordinary while the electronic record behind it shows repeated injections, altered processing methods or deleted runs [6, 7].

1.2 Regulatory scrutiny and enforcement trends

Since about 2013, regulators including the United States Food and Drug Administration (FDA), the European Medicines Agency (EMA) and EU national competent authorities, the United Kingdom Medicines and Healthcare products Regulatory Agency (MHRA), the World Health Organization (WHO) and India's Central Drugs Standard Control Organisation (CDSCO) have given laboratory data integrity far more attention than before [8, 9]. Form FDA 483 observations and warning letters have repeatedly described the same practices: sample preparations that were never recorded, unofficial 'trial' or 'pre-screening' injections, selective reporting of passing results, aborted sequences, unjustified re-integration of chromatographic peaks, and deletion of raw data files that did not meet specification [3, 9].

Problems of this kind are not new. The generic drug scandal of the late 1980s and the 2005 collapse of Able Laboratories, where analysts had manipulated test results, both showed how falsified laboratory records can let unsuitable product reach patients [9]. In 2013 Ranbaxy pleaded guilty to felony charges relating to adulterated drugs and false statements to the FDA and agreed to pay USD 500 million [10, 11]. Beyond financial penalties, import alerts and plant closures, the underlying risk is clinical: sub-potent, degraded or contaminated medicines may be distributed under the cover of compliant-looking paperwork [2, 3]. Regulators therefore now describe data integrity as a basic requirement of Good Manufacturing Practice (GMP) and Good Laboratory Practice (GLP), and expect firms to back it with a data governance system and risk-based oversight [2, 7, 12].

1.3 Rationale and objectives of the review

Data integrity in the QC laboratory sits where analytical chemistry, regulatory science and information technology meet. Analytical method theory and instrumentation are well covered in pharmacy and pharmaceutical science curricula, but the practical controls that make laboratory data defensible, such as computerized system validation, audit trail review and formal risk assessment under ICH Q9(R1), usually receive much less attention [5]. The guidance itself is spread across documents from several agencies, published over twenty-five years, with differing terminology. A single review that brings these sources together and links them to the day-to-day work of an analyst is therefore useful for students, early-career QC staff and quality assurance (QA) reviewers.

The objectives of this review are to:

- compare current data integrity and data governance expectations of the FDA, EMA/European Commission, MHRA, WHO, PIC/S and CDSCO;
- explain how the nine ALCOA+ attributes apply to paper, hybrid and fully electronic laboratory records;
- classify recurring technical, procedural and behavioral failure modes in QC analytical workflows, with emphasis on chromatographic data;

- show how quality risk management (QRM), and failure mode and effects analysis (FMEA) in particular, can be used to prioritize data integrity controls;
- summarize the technical requirements of 21 CFR Part 11 and EU GMP Annex 11, including the shift from conventional computer system validation (CSV) toward computer software assurance (CSA); and
- identify emerging issues, including cloud services and artificial intelligence (AI), that will shape laboratory data integrity in the coming years.

2. METHODOLOGY OF THE REVIEW

This article is a narrative review. Regulatory and standards documents were obtained directly from the websites of the FDA, the European Commission (EudraLex), EMA, MHRA, WHO, the Pharmaceutical Inspection Co-operation Scheme (PIC/S), the International Council for Harmonisation (ICH), the Organisation for Economic Co-operation and Development (OECD) and the Indian Ministry of Health and Family Welfare. Peer-reviewed literature was identified through PubMed, Scopus and Google Scholar using combinations of the terms 'data integrity', 'ALCOA', 'ALCOA+', 'pharmaceutical quality control', 'chromatography data system', 'audit trail', 'quality risk management', 'ICH Q9', 'FMEA', '21 CFR Part 11', 'Annex 11', 'computer system validation' and 'computer software assurance'. Reference lists of retrieved papers and books were also searched by hand.

Documents published between 1997, when 21 CFR Part 11 was issued, and 2025 were considered. Inclusion was limited to English-language guidance that is currently in force or formally released for consultation, peer-reviewed articles, recognized industry guides (ISPE GAMP, PDA technical reports) and specialist textbooks dealing with data integrity, risk management or computerized systems in regulated laboratories. Vendor promotional material and opinion pieces without a regulatory or empirical basis were excluded. Because the aim was to synthesize expectations and practice rather than to estimate an effect size, no formal quality scoring or meta-analysis was performed. Where agencies differ, the differences are reported explicitly.

3. Regulatory framework for data integrity

3.1 Evolution of regulatory expectations

The legal foundation for electronic records in the United States was laid in 1997, when the FDA issued 21 CFR Part 11 on electronic records and electronic signatures [13]. Early implementation proved burdensome, and in 2003 the agency narrowed its interpretation and announced enforcement discretion for several requirements, while keeping the underlying predicate-rule obligations of 21 CFR Parts 210 and 211 [1, 14]. In Europe, Annex 11 on computerised systems and Chapter 4 on documentation were revised in 2011, introducing risk management across the system lifecycle [15, 16].

Data integrity guidance as a separate topic emerged after 2015. The MHRA published a GMP data integrity definitions document in 2015 and replaced it in 2018 with a guidance covering all GxP areas [6]. The EMA released question-and-answer guidance in 2016 [17], WHO issued guidance on good data and record management practices in the same year [18], and the FDA finalized its question-and-answer guidance on data integrity and drug CGMP in December 2018 [3]. PIC/S adopted PI 041-1 for inspectors in 2021 [7], and WHO replaced its 2016 text with a dedicated guideline on data integrity in Technical Report Series No. 1033 [2]. These milestones are summarized in Figure 1.

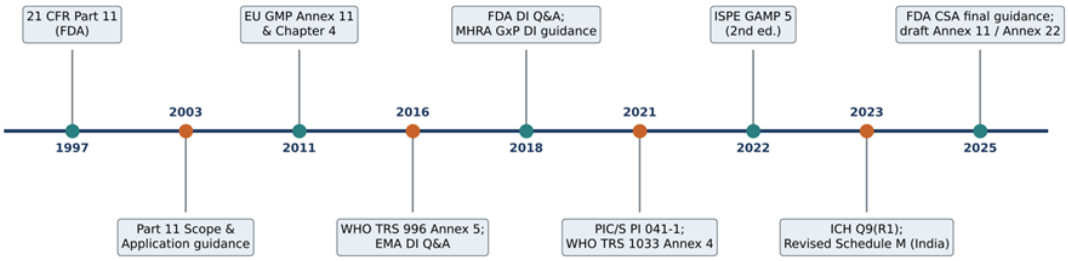


Figure 1. Timeline of major regulatory and industry milestones relevant to data integrity in pharmaceutical quality control laboratories (1997–2025). Compiled from references cited in Section 3.

Industry guidance has developed in parallel. The International Society for Pharmaceutical Engineering (ISPE) published the GAMP Guide on Records and Data Integrity in 2017 and the second edition of GAMP 5 in 2022, which places critical thinking and risk-based assurance at the center of computerized system compliance [19, 20]. The Parenteral Drug Association (PDA) addressed laboratories directly in Technical Report No. 80 [21]. For non-clinical studies, OECD GLP guidance on computerised systems serves a comparable function [22].

More recent changes continue the move toward risk-based thinking. ICH Q9(R1), adopted in January 2023, added text on subjectivity in risk assessment, on the formality of QRM activities and on risk-based decision making [12]. In September 2025 the FDA issued final guidance on computer software assurance for production and quality system software, which encourages testing effort proportional to risk rather than exhaustive scripted documentation [23]. In July 2025 the European Commission opened a stakeholder consultation on revised drafts of Chapter 4 and Annex 11 together with a new Annex 22 on artificial intelligence [24]. In India, the revised Schedule M notified in December 2023 brought domestic GMP requirements closer to WHO and PIC/S standards, including requirements for a pharmaceutical quality system, QRM and computerized systems [25].

3.2 Comparison of key guidance documents

Table 1 compares the main documents. Although their scope and legal status differ, they agree on four core expectations: (i) the ALCOA+ attributes apply to all GxP records regardless of medium; (ii) metadata and audit trails form part of the complete record; (iii) the effort spent on controls should be proportional to data criticality and risk; and (iv) senior management is responsible for creating conditions in which data integrity can be maintained [2, 3, 6, 7].

Table 1. Key regulatory and industry guidance documents on data integrity relevant to QC laboratories.

Agency / body	Document (year)	Scope	Distinctive emphasis
US FDA	21 CFR Part 11 (1997); Part 11 Scope and Application guidance (2003) [13, 14]	Electronic records and signatures required by predicate rules	Controls for closed and open systems; secure, time-stamped audit trails; narrowed interpretation and enforcement discretion after 2003
US FDA	Data Integrity and Compliance with Drug CGMP: Questions and Answers (2018) [3]	Drug CGMP (21 CFR Parts 210, 211, 212)	All CGMP data must be retained, including from 'trial' injections; audit trails reviewed before batch release; testing into compliance is prohibited
European Commission / EMA	EudraLex Vol. 4, Annex 11 and Chapter 4 (2011); EMA data integrity Q&A (2016) [15–17]	EU GMP for human and veterinary medicines	Risk management across the system lifecycle; supplier assessment; periodic evaluation; draft revisions released for consultation in 2025
MHRA (UK)	'GXP' Data Integrity Guidance and Definitions, Rev. 1 (2018) [6]	All GxP areas	Data governance proportional to risk; definitions of raw data, metadata and true copy; static versus dynamic records
WHO	TRS 996 Annex 5 (2016); TRS 1033 Annex 4 (2021) [2, 18]	GxP, including prequalification and national authorities	Management responsibility, QRM, data lifecycle, ALCOA+, controls for hybrid systems
PIC/S	PI 041-1 (2021) [7]	GMP/GDP inspectorates and industry	Detailed expectations for paper and computerized systems; data criticality and data risk; guidance on outsourced activities
CDSCO / MoHFW (India)	Revised Schedule M, G.S.R. 922(E) (2023) [25]	Manufacturers licensed in India	Pharmaceutical quality system, QRM, qualification and validation, and computerized systems aligned with WHO/PIC/S GMP
ICH	Q9(R1) Quality Risk Management (2023); Q10 (2008) [12, 26]	Pharmaceutical quality system	Risk-based decision making; managing subjectivity; formality proportional to risk

Agency / body	Document (year)	Scope	Distinctive emphasis
ISPE / PDA	GAMP 5, 2nd ed. (2022); GAMP RDI Guide (2017); PDA TR 80 (2018) [19–21]	Industry good practice	Critical thinking; data lifecycle; laboratory-specific data integrity management

CGMP, current good manufacturing practice; GDP, good distribution practice; MoHFW, Ministry of Health and Family Welfare; RDI, records and data integrity; TR, technical report; TRS, Technical Report Series.

4. The ALCOA+ framework and metadata governance

4.1 Origin and core principles

The acronym ALCOA (attributable, legible, contemporaneous, original, accurate) is generally attributed to Stan Woollen of the FDA, who used it in the 1990s when teaching GLP inspection [27]. Later guidance added four further attributes: complete, consistent, enduring and available, to give ALCOA+ [2, 17]. Some authors add 'traceable' as a tenth attribute and call the result ALCOA++, but the nine-attribute form is the one used in WHO and PIC/S guidance [2, 7]. The attributes are shown in Figure 2 and described below.



Figure 2. The nine ALCOA+ attributes. The five original ALCOA attributes are shown in dark blue and the four '+' extensions in teal. Based on WHO and PIC/S guidance.

- **Attributable.** Each observation, calculation and system action must be traceable to the person who performed it and, where relevant, the instrument used. On paper this means a signature or initials with date; in software it requires unique user accounts rather than shared or generic log-ins [3, 6].
- **Legible.** Records must remain readable and understandable for the whole retention period. Faded thermal printouts, unclear handwriting and proprietary file formats that can no longer be opened all compromise legibility [2].
- **Contemporaneous.** Data must be recorded when the activity is performed. Completing bench worksheets at the end of a shift or backdating entries makes the record unreliable [2, 3].
- **Original.** The first capture of the data, or a verified true copy, must be retained. This includes notebooks and balance printouts as well as the electronic files holding raw spectra and chromatograms. Writing results on scrap paper before copying them into the official record is a recognized compliance risk [6, 7].
- **Accurate.** Data must be correct and free of unverified changes. Corrections on paper should use a single line through the original entry with the initials, date and reason, leaving the original legible; electronic changes must be captured by the audit trail [2, 16].
- **Complete.** All data, including repeat or invalidated tests, metadata and audit trails, must be retained so that the full history of the analysis can be reconstructed [3, 6].
- **Consistent.** Records should follow a logical, time-ordered sequence, with date and time stamps that agree with each other and with the actual order of events [2].
- **Enduring.** Records must be kept on media that remain intact and readable for the required retention period, whether controlled paper or validated electronic storage [2, 15].
- **Available.** Records must be retrievable for review, audit and inspection throughout their retention period, in a reasonable time [2, 7].

Table 2 shows how each attribute translates into expectations for paper and for electronic or hybrid systems, and lists failures commonly seen in QC laboratories.

Table 2. Application of ALCOA+ attributes to paper and electronic/hybrid QC records.

Attribute	Paper record expectation	Electronic / hybrid expectation	Typical QC failure
Attributable	Signature or initials with date; signature log maintained	Unique user ID and password; e-signature linked to record	Shared 'analyst' or 'admin' account on CDS or UV software
Legible	Permanent ink; controlled forms; no obliteration	Human-readable format retained over retention period	Faded thermal balance slips; obsolete software unable to open files
Contemporaneous	Entries made at time of activity	Server-synchronized time stamps; clock change restricted	Worksheets completed after the shift; PC clock altered

Attribute	Paper record expectation	Electronic / hybrid expectation	Typical QC failure
Original	Bound, issued notebooks and controlled forms	Native raw data files retained, or verified true copies	Results recorded on loose paper; only PDF printouts retained
Accurate	Single-line corrections with reason	Validated calculations; changes captured in audit trail	Unverified spreadsheet calculations; unjustified re-integration
Complete	All pages, repeats and invalidated results retained	Audit trail and metadata retained with data	Deleted 'trial' injections; aborted sequences not reported
Consistent	Chronological entries; no gaps	Sequence, audit trail and instrument logs agree	Injection times that do not match the logbook
Enduring	Archive-quality paper and secure storage	Validated backup and archive; media integrity checks	Data on local hard drive only; no backup verification
Available	Indexed archive; retrieval procedure	Retrieval tested; readable during inspection	Archived data cannot be restored within inspection timeframe

Compiled from FDA (2018), MHRA (2018), PIC/S PI 041-1 (2021) and WHO TRS 1033 Annex 4 (2021).

4.2 Raw data, metadata and the data lifecycle

A printed chromatogram or a single peak area value has little meaning on its own. To show how a result was produced, the reviewer needs its metadata: acquisition and processing method versions, instrument and column identifiers, mobile phase and standard lot numbers, integration parameters, sequence information, time stamps and user identities [5, 6]. The MHRA distinguishes 'static' records, such as a paper printout or an image, from 'dynamic' records, such as a chromatogram that can be re-processed, and states that for dynamic records the electronic form is the original. A paper printout is therefore not an acceptable substitute [6]. The FDA takes the same position for CGMP records [3].

Current guidance treats data integrity as a property to be maintained across the whole data lifecycle, from creation to destruction [2, 19]. Each lifecycle stage carries its own risks and needs its own controls (Figure 3). Interfaces between stages, such as the transfer of results from a CDS to a LIMS, or migration of data when software is upgraded, are especially vulnerable and should be validated [15, 20].

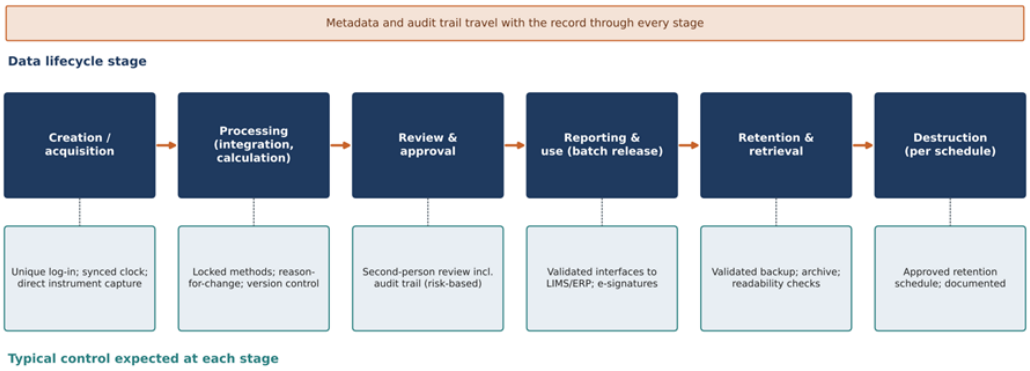


Figure 3. Lifecycle of QC analytical data, with representative controls at each stage. Adapted from concepts in WHO TRS 1033 Annex 4 and the ISPE GAMP Records and Data Integrity Guide.

5. Systemic vulnerabilities in QC analytical workflows

Data integrity failures rarely have a single cause. They usually arise from technical weaknesses that make manipulation possible, procedures that fail to detect it, and an organizational climate that makes it tempting [5, 7]. Table 3 summarizes the failure modes most often reported in inspection findings and the literature.

5.1 Technical weak points

Legacy standalone instruments. Many UV-visible spectrophotometers, FTIR spectrometers, polarimeters and balances in QC laboratories are controlled by stand-alone personal computers running older software. Such systems may have no audit trail, no role-based access, shared log-ins, and data stored in local folders where users can rename, overwrite or delete files [6, 7]. Operating system access often allows the clock to be changed, which undermines every time stamp the system produces. Where replacement is not immediately possible, interim measures include configuring operating-system security, sending data to a secure network location, and adding procedural checks of file folders [5, 7].

Inappropriate privileges. If analysts hold administrator rights on a CDS they can change methods, disable audit trails or delete data. Guidance expects system administration to be separated from routine use, ideally performed by people independent of the laboratory and its results [3, 7].

Unvalidated spreadsheets and interfaces. Spreadsheets used for assay or impurity calculations are computerized systems and need to be controlled and validated. Unlocked cells, unprotected formulas and manual transcription between systems are frequent sources of error [5, 19].

5.2 Procedural weak points

Hybrid workflows and testing into compliance. In hybrid systems data are captured electronically but signed, calculated or reported on paper. If the paper record is treated as the official record, the electronic history behind it may never be reviewed [2, 6]. This gap allows unofficial 'trial' or 'system

suitability' injections of samples, followed by abortion or deletion of runs that show out-of-specification (OOS) results and re-preparation until a passing value is obtained. The FDA states that using actual samples to perform 'test', 'prep' or 'equilibration' runs as a way of disregarding results is a violation, and that all such data must be retained and investigated under the OOS procedure [3, 28].

Misuse of manual integration. Manual adjustment of a baseline can be scientifically justified, for instance with co-eluting peaks or a drifting baseline, but it can also be used to shrink impurity peaks or enlarge assay peaks so that a batch meets specification. Good practice is to define in a procedure when manual integration is permitted, to require a recorded reason, to keep the original integration, and to have a second person review the change in the audit trail [4, 5].

Weak audit trail review. An audit trail that nobody reads deters very little. Common deficiencies are reviews performed only on printed summaries, reviews that do not focus on critical events such as deletions, re-integrations, method changes and aborted runs, and reviews that are not completed before release [3, 7].

Uncontrolled documents. Blank worksheets that can be photocopied freely make it possible to rewrite a record and discard the original. Forms should be issued and reconciled under control [2, 7].

5.3 Organizational and behavioral factors

Technical controls cannot by themselves assure integrity. Where release deadlines are tight and resources thin, small departures from procedure can become accepted practice without anyone deciding that they should. Vaughan's term 'normalization of deviance' describes this process [29]. Under such conditions analysts may avoid raising OOS results, share passwords to save time, or sign logbooks after the event. Reason's work on human error distinguishes slips and mistakes from deliberate violations, and shows that each needs a different response [30]. Honest errors should be reported and corrected without blame, so that real problems surface; deliberate falsification should be handled firmly. Research on psychological safety in work teams shows that people report errors more readily when they do not expect to be punished for doing so [31]. Regulators have taken up these ideas, and both WHO and PIC/S guidance place explicit responsibility on management for workload, resources and an open reporting culture [2, 7].

Table 3. Recurring data integrity failure modes in QC laboratories, likely root causes and suggested controls.

Category	Failure mode	Likely root cause	Preventive / detective control
Technical	Shared or generic log-ins	Licence cost; convenience; legacy software	Unique accounts; role-based access; periodic access review
Technical	Audit trail disabled or not available	Legacy configuration; unvalidated setup	Configuration locked under change control; system upgrade or replacement plan

Category	Failure mode	Likely root cause	Preventive / detective control
Technical	Analysts able to delete or overwrite files	Administrator rights granted to users	Segregation of duties; restricted file system permissions
Technical	Unsynchronized or editable system clock	Stand-alone PC; local OS rights	Network time synchronization; OS lock-down
Procedural	Unreported trial or 'pre-test' injections	Pressure to pass; unclear SOP	Sequence reconciliation; review of all injections and orphan data
Procedural	Unjustified manual re-integration	No integration SOP; weak review	Integration SOP; recorded reason; audit trail review
Procedural	OOS results invalidated without investigation	Inadequate OOS procedure or training	OOS investigation per FDA guidance; QA oversight
Procedural	Transcription errors between systems	Manual data transfer	Direct instrument interfaces; second-person verification
Procedural	Uncontrolled blank forms	Free photocopying of worksheets	Issued and reconciled forms; numbered pages
Behavioral	Backdating or pre-dating entries	Workload; fear of reporting delays	Realistic capacity planning; open reporting; supervision
Behavioral	Concealing errors or failures	Blame culture; incentives tied to output	Psychological safety; quality metrics that reward reporting

Compiled from FDA (2018), MHRA (2018), PIC/S PI 041-1 (2021), McDowall (2019) and Rattan (2018). OS, operating system; SOP, standard operating procedure.

6. Application of quality risk management to data integrity

6.1 Principles of ICH Q9(R1)

Retrospective audits find problems after they have occurred. Quality risk management aims instead to anticipate them. ICH Q9(R1) defines QRM as a systematic process for the assessment, control, communication and review of risks to the quality of the drug product across its lifecycle [12]. Its two primary principles are that the evaluation of risk should be based on scientific knowledge and linked to protection of the patient, and that the level of effort, formality and documentation should be commensurate with the level of risk [12]. The general process is shown in Figure 4.

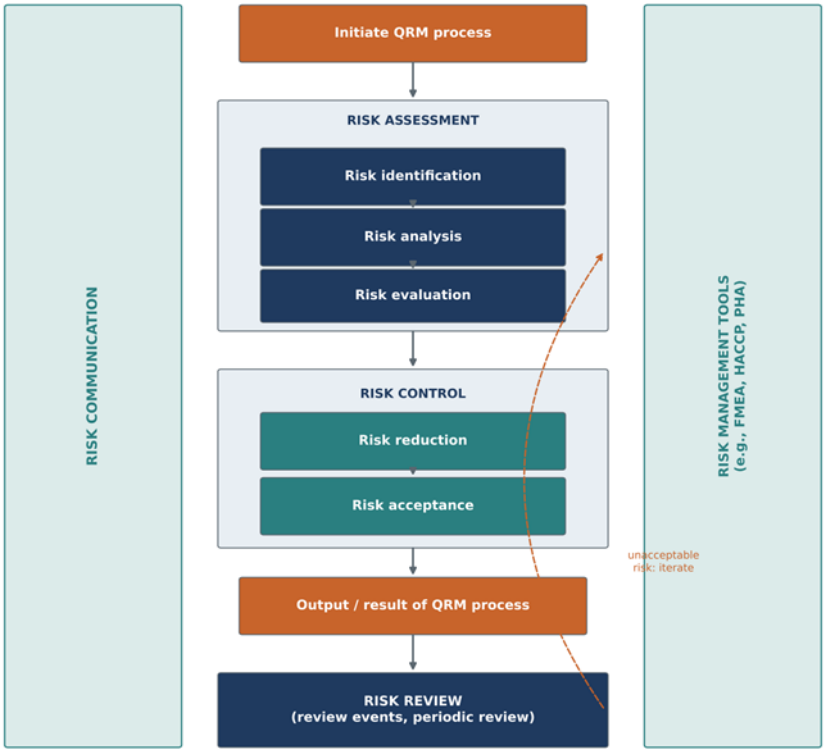


Figure 4. Overview of a typical quality risk management process. Redrawn and simplified from ICH Q9(R1).

The 2023 revision is relevant to data integrity in three ways. First, it acknowledges that risk scores are subjective and asks firms to reduce subjectivity, for example by using cross-functional teams, defined scales and documented rationale [12]. Second, it clarifies that QRM formality can vary, so that a low-risk instrument does not need the same depth of assessment as a CDS. Third, it addresses risk-based decision making and the link between quality problems and product availability [12]. Data integrity guidance builds directly on these ideas: MHRA, PIC/S and WHO all ask firms to assess data criticality, meaning how much a record influences decisions on product quality, and data risk, meaning how vulnerable it is to unauthorized change or loss, and to set controls accordingly [2, 6, 7].

6.2 Failure mode and effects analysis

FMEA is one of the tools listed in ICH Q9(R1) and is widely used in pharmaceutical development and manufacturing [12, 32]. The process to be assessed is broken down into steps; for each step the team identifies how it could fail, what the effect would be, and what currently prevents or detects the failure [33, 34]. Each failure mode is scored, typically on a 1–10 scale, for severity (S), likelihood of occurrence (O) and detectability (D), where a high D score indicates that the failure is hard to detect. The product of the three scores gives the risk priority number (RPN):

RPN = Severity (S) × Occurrence (O) × Detectability (D)

Failure modes with the highest RPNs, or with a high severity score regardless of RPN, are addressed first. After controls are introduced, the scores are re-assessed to confirm that the residual risk is

acceptable [32, 33]. Table 4 gives an illustrative FMEA for an HPLC assay workflow, and Figure 5 compares the RPNs before and after the proposed controls.

Table 4. Illustrative FMEA of data integrity risks in an HPLC assay workflow. (hypothetical scores)

Process step / failure mode	Potential effect	S	O	D	RPN	Recommended control	Revised S/O/D (RPN)
Sample weighing on offline balance; value transcribed incorrectly	Wrong assay result; batch wrongly released or rejected	7	6	8	336	Balance connected to LIMS/CDS; printout attached and second-person verified	7/2/2 (28)
'Trial' sample injections run and deleted before official sequence	OOS result concealed; unsafe batch released	9	5	8	360	Disable deletion rights; reconcile all injections; review orphan data	9/2/2 (36)
Manual re-integration without justification	Impurity under-reported	8	6	7	336	Integration SOP; mandatory reason for change; audit trail review	8/3/3 (72)
Shared analyst log-in on CDS	Actions not attributable	8	5	7	280	Unique accounts; periodic user access review	8/1/2 (16)
Manual transcription of results to LIMS	Reported value differs from raw data	6	6	6	216	Validated electronic interface; verification step	6/2/2 (24)
Incomplete backup of CDS server	Permanent loss of raw data	9	3	7	189	Validated automatic backup; periodic restore test	9/1/3 (27)
Unsynchronized workstation clock	Time stamps unreliable; sequence cannot be reconstructed	6	4	8	192	Network time synchronization; restrict OS clock rights	6/1/2 (12)

Scores are illustrative only and are intended to demonstrate the method; each laboratory must derive its own scores through a documented, cross-functional assessment. S, severity; O, occurrence; D, detectability (10 = least detectable); RPN, risk priority number.

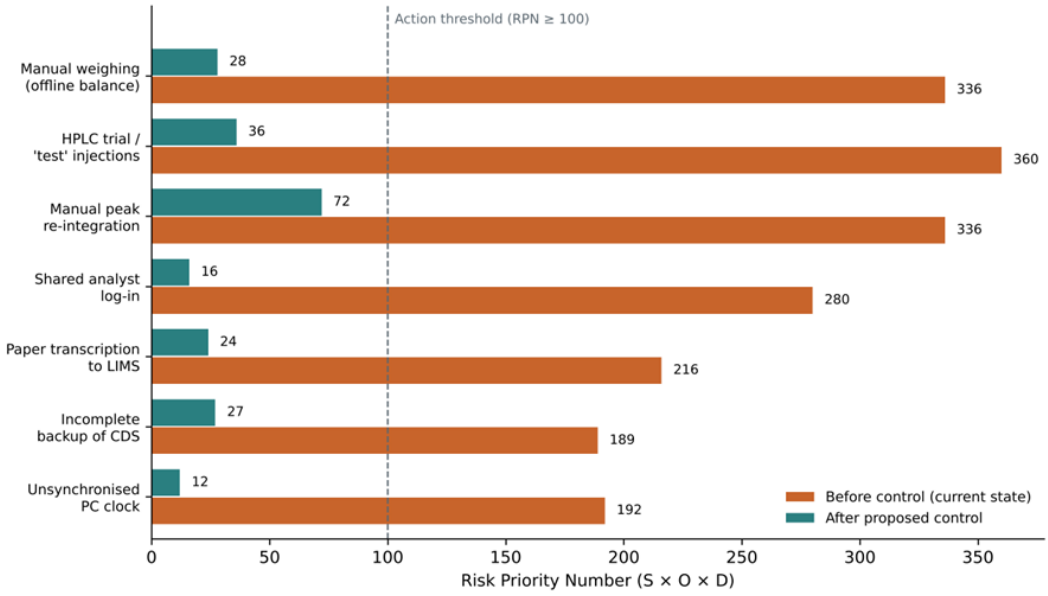


Figure 5. Risk priority numbers for the illustrative FMEA in Table 4 before and after implementation of the recommended controls. The dashed line marks an example action threshold of RPN ≥ 100.

FMEA has known limitations. Different combinations of S, O and D can give the same RPN while representing very different risks, the scales are ordinal so multiplication has limited mathematical meaning, and scores depend heavily on the judgement of the team [35]. These are the concerns that ICH Q9(R1) addresses when it asks firms to manage subjectivity [12]. In practice, laboratories can reduce these weaknesses by defining each score level in writing, by treating any failure mode with high severity as a priority regardless of its RPN, and by recording the rationale for every score.

6.3 Risk-based allocation of controls

Applying QRM lets a laboratory concentrate its effort where data are most critical and most exposed. Systems that generate complex, re-processable data used for batch release, such as CDS and LIMS, require the strongest technical controls and the most frequent review. Simple instruments whose output is a single value that can be verified against a printout need fewer controls [6, 20]. Table 5 illustrates a three-tier approach.

Table 5. Risk-based allocation of data integrity controls to QC laboratory systems.

System risk level	Example QC systems	Expected governance and technical controls	Audit trail review
High	Chromatography data systems (HPLC, UPLC, GC); LIMS; dissolution systems with software processing; enterprise data platforms	Unique user IDs; administrator rights held outside the laboratory; audit trail always on and locked; validated automatic backup and archive; electronic signatures; full lifecycle validation	Review of critical events for every result before release, plus periodic system-level review

System risk level	Example QC systems	Expected governance and technical controls	Audit trail review
Medium	FTIR, UV-visible and NIR software; Karl Fischer titrators with stored data; validated calculation spreadsheets	Role-based access; configuration under change control; data saved to secure network location; risk-based validation	Review focused on changes and deletions, per batch or at defined intervals
Low	pH meters, simple balances and other instruments without stored data or configurable software; calibrated glassware	Qualified and calibrated equipment; printouts attached to the record; controlled logbooks; periodic supervisory review	Not applicable or limited to configuration changes

Classification and frequencies are examples consistent with MHRA (2018), PIC/S PI 041-1 (2021) and GAMP 5 (2nd ed.). Each firm should justify its own classification by documented risk assessment. NIR, near-infrared.

7. Digital compliance, validation and electronic controls

7.1 21 CFR Part 11 and EU GMP Annex 11

The move from paper to electronic records depends on two main texts: 21 CFR Part 11 in the United States and Annex 11 of the EU GMP guide [13, 15]. Part 11 sets out when electronic records and signatures can be considered as trustworthy and reliable as paper records and handwritten signatures. Annex 11 applies more broadly to any computerized system used in GMP activities and puts more emphasis on risk management, supplier assessment and periodic review. Table 6 compares the two.

Table 6. Comparison of 21 CFR Part 11 and EU GMP Annex 11. (2011)

Element	21 CFR Part 11 (US)	EU GMP Annex 11
Legal status	Federal regulation, legally binding	Annex to EU GMP guide, applied through EU GMP directives
Scope	Electronic records and signatures required by predicate rules	All computerized systems used as part of GMP-regulated activities
Risk management	Implied; emphasized in 2003 Scope and Application guidance	Explicit requirement throughout the system lifecycle (Principle and Clause 1)
Validation	§11.10(a): validation to ensure accuracy, reliability and consistent intended performance	Clause 4: lifecycle validation, user requirements, supplier documentation
Audit trail	§11.10(e): secure, computer-generated, time-stamped; changes must not obscure prior entries	Clause 9: based on risk assessment; reason for change documented; audit trails reviewed regularly
Access control	§11.10(d), (g): limited to authorized individuals; authority checks	Clause 12: physical and logical controls; creation and removal of access recorded
Electronic signatures	Subpart C (§§11.50–11.300): manifestation, linking, identification components	Clause 14: same impact as handwritten; permanently linked; time and date

Element	21 CFR Part 11 (US)	EU GMP Annex 11
Suppliers and service providers	Not addressed explicitly	Clause 3: formal agreements; supplier assessment based on risk
Periodic review	Not addressed explicitly	Clause 11: periodic evaluation of validated state
Backup, archiving, continuity	§11.10(c): protection of records for retrieval throughout retention	Clauses 7, 16, 17: backup, business continuity and archiving

Sources: 21 CFR Part 11 (1997), FDA Scope and Application guidance (2003) and EudraLex Vol. 4 Annex 11 (2011). The 2025 consultation draft of Annex 11 proposes more detailed requirements, including on audit trail review and cloud services.

7.2 From computer system validation to computer software assurance

Validation demonstrates that a computerized system does what it is intended to do, consistently and reliably [13, 15]. GAMP 5 classifies software by its degree of configuration and customization and scales validation effort accordingly; a configured CDS (category 4) needs more work than non-configured standard software (category 3), and bespoke code (category 5) needs the most [20]. Laboratory instruments are also qualified, for example under USP general chapter <1058>, so that instrument qualification and software validation together establish fitness for use [36].

A common criticism of traditional CSV is that it produced large amounts of scripted test evidence for low-risk functions while sometimes testing high-risk functions poorly. Both the second edition of GAMP 5 and the FDA's 2025 CSA guidance respond to this by encouraging critical thinking: identifying the intended use, determining which functions could affect product quality or data integrity, and concentrating rigorous testing there, while using unscripted or exploratory testing and supplier evidence for lower-risk functions [20, 23]. The CSA guidance was written for medical device production and quality system software, but its principles are consistent with ICH Q9(R1) and are being applied more widely [12, 23].

7.3 Access control and audit trails

Role-based security should ensure that analysts cannot alter system clocks, change processing methods outside change control, disable audit trails or delete data [3, 7]. User accounts should be personal, passwords should not be shared, and user lists should be reviewed periodically to remove leavers and correct privileges.

The audit trail is a secure, computer-generated, time-stamped record that allows reconstruction of the creation, modification and deletion of an electronic record [3, 13]. Because a paper printout conceals what happened inside the software, the FDA expects audit trails that capture changes to critical data to be reviewed with each record and before final approval [3]. In practice, effective review targets events that could change a reportable result, such as re-integration, re-processing, changes to methods or sequences, aborted runs and deletions. Reviewing every line of an audit trail is neither feasible nor

useful [5, 7]. Review-by-exception reports, which highlight only such events, make routine review practical, provided the report itself has been validated [19].

7.4 Backup, archiving and data migration

Electronic records must be backed up at a frequency based on risk, and the restore process must be tested periodically, not only the backup [2, 15]. Archived data must remain readable, which may require keeping old software versions, converting files with verified true-copy procedures, or using vendor-neutral formats. Data migration during system upgrades or replacement must be validated so that records, metadata and audit trails remain complete and linked [2, 20].

7.5 Outsourced and cloud-hosted systems

Laboratories increasingly use LIMS, electronic laboratory notebooks and CDS hosted by vendors or provided as software-as-a-service. The regulated company remains responsible for data integrity in these arrangements [7, 15]. Supplier assessment, quality agreements that define responsibility for backup, security, audit trail retention and data return at contract end, and evidence that the hosting environment is controlled, are therefore essential. The 2025 Annex 11 consultation draft addresses cloud services in more detail than the 2011 text [24].

8. Data governance and quality culture

Data governance is the sum of arrangements that ensure data, whatever their format, are recorded, processed, retained and used in a way that gives a complete, consistent and accurate record throughout the data lifecycle [6]. It has three layers that depend on each other (Figure 6). Technical controls make manipulation difficult and detectable. Procedural and organizational controls define responsibilities, training and review. Management behavior and quality culture determine whether people follow the procedures when under pressure [2, 7, 26].



Figure 6. Layered model of data governance in the QC laboratory. Each layer supports the one below; trustworthy data depend on all three.

Senior management's role is explicit in recent guidance. Managers are expected to provide sufficient staff and equipment, to set realistic schedules, to avoid targets that reward speed at the expense of quality, and to respond to reported errors in a way that encourages further reporting [2, 7]. ICH Q10 places similar responsibility on management for the pharmaceutical quality system as a whole [26]. Useful practical measures include data integrity training based on real case studies, clear designation of data owners for each system, periodic data integrity audits that include unannounced review of raw electronic data, and quality metrics such as invalidated OOS rates, numbers of re-injections and frequency of manual integration, which can signal emerging problems [5, 21].

When a data integrity problem is found, guidance expects a structured response: a comprehensive investigation of its scope, an assessment of its effect on released product, a management strategy with corrective and preventive actions, and, where appropriate, notification of regulators [3]. Remediation is likely to fail if it addresses only the technical symptom, for example by enabling an audit trail, without examining why the behavior arose [9].

9. Emerging trends and future perspectives

Pharma 4.0 and integrated data flows. Laboratories are moving toward connected systems in which instruments, CDS, LIMS and enterprise resource planning software exchange data without manual transcription. Integration of this kind removes many of the transcription and hybrid-record risks described above, but it concentrates risk in interfaces and master data, which must be validated and monitored [37, 38].

Automated audit trail analytics. Software that analyzes audit trails across many runs can detect patterns that a reviewer looking at one batch will miss, such as unusually frequent re-integration by one user or repeated aborted sequences on one instrument. Such tools can make audit trail review both more efficient and more effective, provided they are validated and their limitations are understood [19, 37].

Artificial intelligence and machine learning. AI is beginning to be used for peak integration, spectral interpretation, anomaly detection and trend analysis. These uses raise new questions about the validation of models that learn from data, the traceability of AI-generated outputs, and human oversight. The FDA has published a discussion paper on AI in drug manufacturing [39], the EMA has issued a reflection paper on AI across the medicinal product lifecycle [40], and the European Commission's draft Annex 22 proposes GMP requirements for AI models used in critical applications [24]. For QC laboratories, ALCOA+ will have to be extended to training data, model versions and decision logs.

Blockchain and distributed ledgers. Distributed ledger technology has been proposed as a way to make records tamper-evident and to provide end-to-end traceability of manufacturing data. Pilot work in pharmaceutical manufacturing is promising, but questions of validation, performance, integration with existing systems and regulatory acceptance remain [41].

10. Challenges, research gaps and limitations

Several difficulties remain. Many laboratories, particularly small and medium-sized manufacturers, still depend on legacy instruments that cannot meet current expectations without costly replacement. Guidance from different agencies uses different terminology and, in places, different levels of detail, which complicates compliance for firms that supply several markets. Published empirical evidence on which controls most effectively reduce data integrity failures is scarce. Most literature consists of guidance, expert opinion and analyses of inspection findings rather than controlled studies [8, 9]. Studies that measure the effect of specific interventions, such as review-by-exception tools, cultural programs or CSA-based validation, on inspection outcomes would be valuable. Standardized and validated approaches to scoring data integrity risk, which respond to the subjectivity concern raised in ICH Q9(R1), are also needed [12, 35].

This review has limitations. It is narrative rather than systematic, so the selection of literature may reflect the authors' judgement. It concentrates on chemical QC testing; microbiological laboratories present additional issues, such as plate reading and colony counting, that are only touched on here. Regulatory documents change regularly, and the draft revisions of Annex 11 and Chapter 4 and the new Annex 22 may change before adoption. Readers should consult the current versions.

11. CONCLUSION

Data integrity in pharmaceutical QC laboratories has moved from a specialist topic to a central element of GMP compliance. The guidance issued by the FDA, EMA, MHRA, WHO, PIC/S and CDSCO differs in emphasis but agrees on the essentials: records must meet the ALCOA+ attributes throughout their lifecycle, metadata and audit trails form part of the record, and controls should be proportional to the criticality and vulnerability of the data. Recurring failures, including shared log-ins, unreported trial injections, unjustified manual integration and superficial audit trail review, have technical, procedural and behavioral causes, and each type of cause needs its own remedy. Quality risk management under ICH Q9(R1), using tools such as FMEA with appropriate attention to subjectivity, offers a structured way to decide where effort should go. Compliance with 21 CFR Part 11 and EU GMP Annex 11, supported by risk-based assurance, addresses the technical layer. Lasting improvement, however, depends on management that provides adequate resources and a culture in which analysts can report problems without fear. As laboratories adopt integrated platforms, cloud services and AI, the same principles will apply, extended to new kinds of data. Teaching these principles explicitly in pharmacy and pharmaceutical science education would help prepare graduates for that work.

Declarations

Acknowledgements: The authors thank [names/institution] for their support.

Author contributions: [Author 1]: conceptualization, literature search, writing – original draft. [Author 2]: literature search, preparation of tables and figures. [Author 3]: supervision, writing – review and editing. All authors read and approved the final manuscript.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors.

Conflict of interest: The authors declare no conflict of interest.

Ethics approval: Not applicable. This review is based on published literature and publicly available regulatory documents and did not involve human participants or animals.

Data availability: No new data were generated or analyzed in this study. The FMEA scores in Table 4 and Figure 5 are illustrative.

REFERENCES

1. U.S. Food and Drug Administration. Code of Federal Regulations, Title 21, Part 211: Current good manufacturing practice for finished pharmaceuticals. Washington, DC: U.S. Government Publishing Office; [cited 2026 Oct 29]. Available from: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211
2. World Health Organization. Guideline on data integrity. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fifty-fifth report. Geneva: World Health Organization; 2021. Annex 4 (WHO Technical Report Series, No. 1033).
3. U.S. Food and Drug Administration. Data integrity and compliance with drug CGMP: questions and answers. Guidance for industry. Silver Spring, MD: FDA, Center for Drug Evaluation and Research; December 2018.
4. McDowall RD. Validation of chromatography data systems: ensuring data integrity, meeting business and regulatory requirements. 2nd ed. Cambridge: Royal Society of Chemistry; 2017.
5. McDowall RD. Data integrity and data governance: practical implementation in regulated laboratories. Cambridge: Royal Society of Chemistry; 2019.
6. Medicines and Healthcare products Regulatory Agency. 'GXP' data integrity guidance and definitions. Revision 1. London: MHRA; March 2018.
7. Pharmaceutical Inspection Co-operation Scheme. Good practices for data management and integrity in regulated GMP/GDP environments. PI 041-1. Geneva: PIC/S; 1 July 2021.
8. Shafiei N, De Montardy R, Rivera-Martinez E. Data integrity—a study of current regulatory thinking and action. PDA J Pharm Sci Technol. 2015;69(6):762–70.
9. Rattan AK. Data integrity: history, issues, and remediation of issues. PDA J Pharm Sci Technol. 2018;72(2):105–16. doi:10.5731/pdajpst.2017.007765
10. U.S. Department of Justice, Office of Public Affairs. Generic drug manufacturer Ranbaxy pleads guilty and agrees to pay $500 million to resolve false claims allegations, cGMP violations and false statements to the FDA [press release]. Washington, DC: DOJ; 13 May 2013.
11. Eban K. Bottle of lies: the inside story of the generic drug boom. New York: Ecco; 2019.
12. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH harmonised guideline Q9(R1): quality risk management. Geneva: ICH; 18 January 2023.
13. U.S. Food and Drug Administration. 21 CFR Part 11: Electronic records; electronic signatures. Final rule. Fed Regist. 1997 Mar 20;62(54):13430–66.
14. U.S. Food and Drug Administration. Guidance for industry. Part 11, electronic records; electronic signatures—scope and application. Rockville, MD: FDA; August 2003.
15. European Commission. EudraLex Volume 4: EU guidelines for good manufacturing practice for medicinal products for human and veterinary use. Annex 11: Computerised systems. Brussels: European Commission; 2011.

16. European Commission. EudraLex Volume 4: EU guidelines for good manufacturing practice for medicinal products for human and veterinary use. Part I, Chapter 4: Documentation. Brussels: European Commission; 2011.
17. European Medicines Agency. Questions and answers: good manufacturing practice—data integrity. London: EMA; August 2016.
18. World Health Organization. Guidance on good data and record management practices. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fiftieth report. Geneva: World Health Organization; 2016. Annex 5 (WHO Technical Report Series, No. 996).
19. International Society for Pharmaceutical Engineering. GAMP guide: records and data integrity. Tampa, FL: ISPE; 2017.
20. International Society for Pharmaceutical Engineering. GAMP 5: a risk-based approach to compliant GxP computerized systems. 2nd ed. Tampa, FL: ISPE; 2022.
21. Parenteral Drug Association. Technical report No. 80: data integrity management system for pharmaceutical laboratories. Bethesda, MD: PDA; 2018.
22. Organisation for Economic Co-operation and Development. Application of GLP principles to computerised systems. OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 17. Paris: OECD Publishing; 2016.
23. U.S. Food and Drug Administration. Computer software assurance for production and quality system software. Guidance for industry and Food and Drug Administration staff. Silver Spring, MD: FDA; September 2025.
24. European Commission. EudraLex Volume 4: draft revision of Chapter 4 (Documentation), Annex 11 (Computerised systems) and new Annex 22 (Artificial intelligence). Stakeholders' consultation. Brussels: European Commission; July 2025.
25. Ministry of Health and Family Welfare, Government of India. Drugs Rules, 1945: Schedule M—good manufacturing practices and requirements of premises, plant and equipment for pharmaceutical products. G.S.R. 922(E). The Gazette of India, Extraordinary; 28 December 2023.
26. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH harmonised tripartite guideline Q10: pharmaceutical quality system. Geneva: ICH; 2008.
27. Woollen SW. Data quality and the origin of ALCOA. The Compass: Newsletter of the Southern Regional Chapter of the Society of Quality Assurance. 2010 Summer.
28. U.S. Food and Drug Administration. Investigating out-of-specification (OOS) test results for pharmaceutical production. Guidance for industry. Revision 1. Silver Spring, MD: FDA; May 2022.
29. Vaughan D. The Challenger launch decision: risky technology, culture, and deviance at NASA. Chicago: University of Chicago Press; 1996.

30. Reason J. Human error. Cambridge: Cambridge University Press; 1990.
31. Edmondson A. Psychological safety and learning behavior in work teams. Adm Sci Q. 1999;44(2):350–83. doi:10.2307/2666999
32. Charoo NA, Ali AA. Quality risk management in pharmaceutical development. Drug Dev Ind Pharm. 2013;39(7):947–60. doi:10.3109/03639045.2012.699065
33. Stamatis DH. Failure mode and effect analysis: FMEA from theory to execution. 2nd ed. Milwaukee, WI: ASQ Quality Press; 2003.
34. International Electrotechnical Commission. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). Geneva: IEC; 2018.
35. Liu HC, Liu L, Liu N. Risk evaluation approaches in failure mode and effects analysis: a literature review. Expert Syst Appl. 2013;40(2):828–38. doi:10.1016/j.eswa.2012.08.010
36. United States Pharmacopeial Convention. General chapter <1058> Analytical instrument qualification. In: United States Pharmacopeia and National Formulary (USP–NF). Rockville, MD: USP; current official edition.
37. Alosert H, Savery J, Rheaume J, Cheeks M, Turner R, Spencer C, et al. Data integrity within the biopharmaceutical sector in the era of Industry 4.0. Biotechnol J. 2022;17:e2100609. doi:10.1002/biot.202100609
38. Steinwandter V, Borchert D, Herwig C. Data science tools and applications on the way to Pharma 4.0. Drug Discov Today. 2019;24(9):1795–805. doi:10.1016/j.drudis.2019.06.005
39. U.S. Food and Drug Administration, Center for Drug Evaluation and Research. Artificial intelligence in drug manufacturing. Discussion paper. Silver Spring, MD: FDA; 2023.
40. European Medicines Agency. Reflection paper on the use of artificial intelligence (AI) in the medicinal product lifecycle. EMA/CHMP/CVMP/83833/2023. Amsterdam: EMA; September 2024.
41. Leal F, Chis AE, Caton S, et al. Smart pharmaceutical manufacturing: ensuring end-to-end traceability and data integrity in medicine production. Big Data Res. 2021;24:100172. doi:10.1016/j.bdr.2020.100172