序号	法规/指南名称 版本号/发布时间	所属章节	内容	分类
1	中国-《药品生产质量管理规范》 2010 年修订	NA	NA	NA
2	中国-《药品生产质量管理规范》 附录：计算机化系统 2015 年	NA	NA	NA
3	中国-《药品记录与数据管理要求（试行）》 2020 年	NA	NA	NA
4	中国-《疫苗生产检验电子化记录技术指南（试行）》 2022 年	NA	NA	NA
5	FDA-21 CFR Part 11 Electronic Records; Electronic Signatures 2023 年	NA	NA	NA
6	FDA-Data Integrity and Compliance with CGMP Q&A 2018 年	NA	NA	NA
7	EU-GMP Annex 11 Computerised Systems 2011 年	NA	NA	NA
8	EU-GMP Annex 11 Concept Paper on the Revision of Annex 11 2022 年	NA	NA	NA
9	EMA-Data Integrity Q&A 2016 年	NA	NA	NA
10	EMA-Guideline on Computerised Systems and Electronic Data in Clinical Trials 2023 年	NA	NA	NA
11	MHRA-GXP Data Integrity Guidance and Definitions 2018 年	6.13	Audit Trail Where relevant audit trail functionality does not exist (e.g. within legacy systems) an alternative control may be achieved for example defining the process in an	Ⅰ、Ⅱ

			SOP, and use of log books. Alternative controls should be proven to be effective. Where add-on software or a compliant system does not currently exist, continued use of the legacy system may be justified by documented evidence that a compliant solution is being sought and that mitigation measures temporarily support the continued use.	
		6.17.1	Archive Archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of archiving of electronic data, this process should be validated, and in the case of legacy systems the ability to review data periodically verified (i.e. to confirm the continued support of legacy computerised systems). Where hybrid records are stored, references between physical and electronic records must be maintained such that full verification of events is possible throughout the retention period. When legacy systems can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes (for as long possible depending upon the specific retention requirements). This may be achieved by maintaining software in a virtual environment.	II
12	ICH-E6(R3)《药物临床试验质量管理规范（草案）》 2023 年	NA	NA	NA
13	ISPE-GAMP5 第二版 A Risk-Based Approach to Compliant GxP Computerized Systems 2022 年	18.3.2.3	Appendix M10 – System Retirement System Retirement Planning Contents of the System Retirement Plan Overview and Implications Consideration should be given to the effect of system retirement on aspects such as: • Strategy – Document the impact on the overall technology strategy to include archive access controls, including further viewing of the data (and, in the case of dynamic data, reprocessing if required), and initiate any updates to documentation or other necessary actions. For example, in order to access and use archived data, the strategy may require the retention of software, inclusive of	II

			licenses, and hardware with appropriate operating system to support the use of the software. ISPE GAMP RDI Good Practice Guide: Data Integrity by Design [36] contains extensive guidance on maintaining data readability (Section 3.2), managing inactive data in an archive (Section 7.2) and the challenges of maintaining legacy software (Appendix O5).	
		20.3.10	Appendix M12 – Critical Thinking Guidance Retirement Retirement is the last of the system life cycle phases and consists of withdrawal, decommissioning, and disposal. Data may be retained for a period in its original system for reading, migrated to a new replacement system, or migrated to another system for archive. Critical thinking and risk management are needed to effectively evaluate what data needs to be retained, for what period of time, and how, such as: • Balancing the risk of data migration against the complexity of maintaining a legacy copy of the system. • Retaining legacy systems as a long-term solution to record readability because systems and software become obsolete over time.	II
		45.4.7	Appendix O13 – Archiving and Retrieval Guidance Retaining Existing Systems On occasions, historical records may be retained in an existing system to support records retention. For example, following the upgrade to a new solution, only current records may be migrated to the new solution and historical records may be retained in the existing solution. In such cases, the DAP must consider: • Ensuring that hardware and software are available to support the legacy application	II
14	WHO-TRS 1033 Annex 4 Guideline on Data Integrity 2021 年	6.2	Management review The acquisition of non-compliant computerized systems and software should be avoided. Where existing systems do not meet current requirements, appropriate controls should be identified and implemented based on risk assessment.	II
		11.9	Computerized systems	II

			Access and privileges For systems generating, amending or storing GxP data, shared logins or generic user access should not be used. The computerised system design should support individual user access. Where a computerised system supports only a single user login or limited numbers of user logins and no suitable alternative computerised system is available, equivalent control should be provided by third-party software or a paper-based method that provides traceability (with version control). The suitability of alternative systems should be justified and documented. The use of legacy hybrid systems should be discouraged and a priority timeline for replacement should be established.	
		11.12	Audit trail Where a system cannot support ALCOA+ principles by design (e.g. legacy systems with no audit trail), mitigation measures should be taken for defined temporary periods. For example, add-on software or paper-based controls may be used. The suitability of alternative systems should be justified and documented. This should be addressed within defined timelines.	II
15	PDA-No.80 Data Integrity Management System for Pharmaceutical Laboratories 2018 年	6.3.9.4	Data Integrity in the Analytical Quality Control Laboratory Analytical Laboratory Computerized Systems (ALCS) Audit Trails Results Audit Trail Filters can also be used to search the requirement from huge amounts of data. Figure 6.3.9.4-2 represents a filter to search whether the sample has been injected in multiple projects. For older systems with limited functionality, the reviewer should sign and stamp results printed on paper and review the electronic data according to the Quality Unit policy. If the results are published electronically, the reviewer should e-sign the results after reviewing and lock the signed file. If it will be used for any investigational purpose, the Quality Unit must review the electronic data per the firm's policy, as electronic data is deemed to be final. Once the printed data is audited, original electronic data should be available for reference and should not be altered. Any modification to the approved data needs to be justified.	II

		6.3.10.1	Transactional Log/System Errors Chromatography The Quality Unit for the lab must establish and validate error messages during equipment installation and qualification. Some error messages are specific to the operating system of the software and are not directly related to data or equipment operation. It is important to work with the software supplier to understand the description of messages that are recorded in the transactional log as they may be subject to evaluation during inspection. Further, it is important to identify those messages that are critical, i.e., related to data and instrument operations. For existing or previously installed equipment (e.g., legacy systems), during installation and qualification, the Quality Unit should assure that all transactional log messages are reviewed and understood, and that critical messages are identified and included in validated audit trails. Transactional log messages that have no impact on analyses or quality attributes of a product and messages that are also recorded in validated audit trails need not be retained.	II
		6.3.11	Common Deficiencies The following problems, listed with the respective ALCS components, are often encountered and commonly found in audits or cited in FDA Warning Letters: • Off-the-Shelf Software - Software version changes incompatible with older files	II
		6.5.1	Laboratory Data Management Software Controls The following are the minimum controls needed to validate laboratory data management software: • Maintain copies of older versions of software whenever version is updated (recommended) and ensure that backed-up data from previous versions can still be accessed	II
16	PIC/S 041-1-Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments 2021 年	9.1.4	SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS Structure of the Pharmaceutical Quality System and control of computerised systems The processes for the design, evaluation, and selection of computerised systems	I 、II

			should include appropriate consideration of the data management and integrity aspects of the system. Regulated users should ensure that vendors of systems have an adequate understanding of GMP/GDP and data integrity requirements, and that new systems include appropriate controls to ensure effective data management. Legacy systems are expected to meet the same basic requirements; however, full compliance may necessitate the use of additional controls, e.g. supporting administrative procedures or supplementary security hardware/software.	
		9.1.7	Consideration should be given to the inherent data integrity controls incorporated into the system and/or software, especially those that may be more vulnerable to exploits than more modern systems that have been designed to meet contemporary data management requirements. Examples of systems that may have vulnerabilities include: manual recording systems, older electronic systems with obsolete security measures, non-networked electronic systems and those that require additional network security protection e.g. using firewalls and intrusion detection or prevention systems.	I
		9.3.1	Validation and Maintenance Expectation Legacy systems (existing systems in use) should be evaluated to determine whether existing system configuration and functionality permits the appropriate control of data in accordance with good data management and integrity practices. Where system functionality or design of these systems does not provide an appropriate level of control, additional controls should be considered and implemented. Potential risk of not meeting expectations/items to be checked • Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection.	II
		9.3.6	Expectation Operating systems and network components (including hardware) should be	II 、III

			updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conducted in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system. Security patches for operating systems and network components should be applied in a controlled and timely manner according to vendor recommendations in order to maintain data security. The application of security patches should be performed in accordance with change management principles. Where unsupported operating systems are maintained, i.e. old operating systems are used even after they run out of support by the vendor or supported versions are not security patched, the systems (servers) should be isolated as much as possible from the rest of the network. Remaining interfaces and data transfer to/from other equipment should be carefully designed, configured and qualified to prevent exploitation of the vulnerabilities caused by the unsupported operating system. Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks. Potential risk of not meeting expectations/items to be checked • Verify that system updates are performed in a controlled and timely manner. Older systems should be reviewed critically to determine whether appropriate data integrity controls are integrated, or, (where integrated controls are not possible) that appropriate administrative controls have been implemented and are effective.	
		9.4.2	Data Transfer Expectation Where conversion to the new data format of the new software is not possible, the old software should be maintained, e.g. installed in one computer or other technical solution, and also available as a backup media in order to have the opportunity to read the archived data in case of an investigation.	II
		9.4.3	Expectation When legacy systems software can no longer be supported, consideration should	II

			be given to maintaining the software for data accessibility purposes (for as long possible depending upon the specific retention requirements). This may be achieved by maintaining software in a virtual environment. Migration to an alternative file format that retains as much as possible of the 'true copy' attributes of the data may be necessary with increasing age of the legacy data.	
		9.5.1	System security for computerised systems Potential risk of not meeting expectations/items to be checked • It is acknowledged that some legacy computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third party software, or a paper-based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems.	II
		9.6.1	Audit trails for computerised systems Expectation Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality.	II
17	APIC-Practical Risk-Based Guide for Managing Data Integrity 2022 年	NA	NA	NA
18	ECA-GMP, GCP and GDP Data Governance and Data Integrity 2022 年	8.7	Illustrative Appendices Hybrid Systems Hybrid systems where both paper and electronic records exist and are kept are much discouraged and possess a threat to data integrity. However, there are some systems, such as legacy systems were this is unavoidable. In that case, mitigating controls should be in place. 8.7.1 Record Types in Hybrid Systems There are several types of hybrid records: • Records obtained from the processing of physical observations such as processing of SDS-PAGE and other in-gel techniques. • Records obtained/originated directly from stand-alone computerized	I 、 II

			instruments such as spectrophotometers and FT-IR. • Records obtained from fully electronic computerized systems but firms have defined paper as raw data. A corollary is where a laboratory used instruments that has the capability to capture and store electronic data but paper was the only record was subject to an FDA warning letter. The last type has no place in current GMP requirements. The first two types of hybrid records are often created by legacy systems. This kind of analytical instruments and systems often have generic logon, lack audit trails and features for electronic signatures. One of the first problems with legacy system is that they usually have shared or generic logon credentials. Thus, actions on electronic records cannot be attributable. A possible mitigation would be to establish signatures on paper records or a logbook of actions and persons that accessed the system. This is not ideal and such systems should be identified for replacement as soon as possible.	
		8.8.1	Spreadsheets Data integrity model for spreadsheet templates • Where relevant audit trail functionality does not exist (e.g. within legacy systems and spreadsheets) an equivalent level of control may be achieved for example by the use of log books, protecting each version and change control	II
19	中国-《血液制品生产检验电子化记录技术指南（试行）》 2024 年	NA	NA	NA