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	第二十一条	应当建立系统出现故障或损坏时进行处理的操作规程，必要时对该操作规程的相关内容进行验证。 包括系统故障和数据错误在内的所有事故都应当被记录和评估。重大的事故应当进行彻底调查，识别其根本原因，并采取相应的纠正措施和预防措施。	Ⅰ、Ⅱ
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	5.3.2	建议通过扫描物料标签上编码的方式对物料的称量、配料、转移、接收、贮存和使用进行电子化记录，辅助进行物料识别，避免混淆和差错。 记录生产过程的物料平衡，综合理论用量，计算物料平衡率，建议如果超出偏差范围，给予异常提醒。	Ⅰ
		5.4.2	电子批记录的生产部分至少要包含以下内容： i）对特殊问题或异常事件的电子记录，包括对偏离工艺规程的偏差情况的详细说明，并经授权人员的电子签名批准。 生成电子批记录的信息系统，应当根据生产过程控制要求，监控特定的关键工艺参数是否符合要求，不符合要求时生成报警或异常事件。	Ⅰ、Ⅲ
		5.4.3	应当根据预设的标准自动捕获或人工记录异常情况，经确认为质量偏差的，根据工艺规程和操作 SOP 中的规定记录生产过程中产生的偏差相关的电子数据，包括但不限于偏差事件描述、发生时间、紧急处理措施、受影响批次、偏差记录人和复核人。	Ⅰ
		5.4.5	电子批包装记录至少要包含以下内容： i）对特殊问题或异常事件的电子记录，包括对偏离工艺规程的偏差情况的详细说明，并经授权人员的电子签名批准；	Ⅰ
		5.4.6	电子批生产记录和批包装记录应当具有筛选排序功能，可便捷查看涉及异常报警或偏差的工序和批次，提升质量管理部门对批生产记录和批包装记录的审核效率。 所有与该批产品有关的异常报警和偏差均已有明确的解释或说明，或者已经过彻底调查和适当处理，在电子批记录中形成明确的结论，并经相关授权人员的电子签名后批准成品放行。 应当对电子批生产记录进行审核，审核内容主要包括：批次生产过程数据、偏差、异常数据处理及数据修改日志，QA（Quality Assurance，质量保证）审核意见。	Ⅰ、Ⅱ
		5.5	建议记录空调净化系统和生产区监控数据的报警信息，包括报警发生的时间、位置信息、设备信息、报警内容、处理人和恢复时间等电子数据，并允许查询和打印报警信息。	Ⅳ
		5.6	建议记录水系统报警发生的时间、设备信息、报警内容、处理人、处理方法和恢复时间等电子数据， 并允许查询和打印报警信息。	Ⅳ
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	1. a	Data integrity is critical throughout the CGMP data life cycle, including in the creation, modification, processing, maintenance, archival, retrieval, transmission, and disposition of data after the record's retention period ends. 6 System design and controls should enable easy detection of errors, omissions, and aberrant results throughout the data's life cycle.	Ⅰ
		8 Remark 13	Risks to data include, but are not limited to, the potential to be deleted, amended, or excluded without authorization or without detection. Examples of audit trails that may be appropriate to review on a risk-based frequency include audit trails that capture instrument operational status, instrument communication logs, and alert records.	Ⅱ
		13	If an actual sample is to be used for system suitability testing, it should be a properly characterized secondary standard, written procedures should be established and followed, and the sample should be from a different batch than the sample(s) being tested (§§ 211.160, 211.165, and 212.60). CGMP original records must be complete (e.g., §§ 211.68(b), 211.188, 211.194) and subjected to adequate review (§§ 211.68(b), 211.186(a), 211.192, and 211.194(a)(8)). Transparency is necessary. All data—including obvious errors and failing, passing, and suspect data—must be in the CGMP records that are retained and subject to review and oversight. An investigation with documented, scientifically sound justification is necessary for data to be invalidated and not used in determining conformance to specification for a batch (see §§ 211.160, 211.165, 211.188, and 211.192).	Ⅰ
7	EU-GMP Annex 11 Computerised Systems 2011 年	4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	Ⅱ
		11	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Ⅱ
		13	Incident Management All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Ⅱ
8	EU-GMP Annex 11 Concept Paper on the Revision of Annex 11 2022 年	22	[9] Guidelines for acceptable frequency of audit trail review should be provided. For audit trails on critical parameters, e.g. setting of alarms in a BMS systems giving alarms on differential pressure in connection with aseptic filling, audit trail reviews should be part of batch release, following a risk-based approach.	Ⅱ、Ⅳ
		24	[9] It should be addressed that many systems generate a vast amount of alarms and event data and that these are often mixed up with audit trail entries. While alarms and events may require their own logs, acknowledgements and reviews, this should not be confused with an audit trail review of manual system interactions. Hence, as a minimum, it should be possible to be able to sort these.	Ⅳ
9	EMA-Data Integrity Q&A 2016 年	9	This is a particular consideration where computerised systems alert the user to an out of specification entry before the data entry process is complete (i.e. the user 'saves' the data entry), or saves the record in temporary memory.	Ⅳ
10	EMA-Guideline on Computerised Systems and Electronic Data in Clinical Trials 2023 年	A5.1.1.1	It should be considered to include a scheduling/calendar component with alerts or reminders to assist compliance.	Ⅰ
		A5.3.10	There should be procedures and processes in place for a trial participant to be able to withdraw their consent. If there is a possibility for the trial participant to withdraw from the trial through the computerised system, it should be ensured that such a withdrawal of consent generates an alert to the investigator in order to initiate the relevant steps as per protocol and according to the extent of withdrawal. Any withdrawal of informed consent should not affect the results of activities already carried out, such as the storage and use of data obtained on the basis of informed consent before withdrawal.	Ⅲ
11	MHRA-GXP Data Integrity Guidance and Definitions 2018 年	NA	NA	NA
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	11.5.5	Controls for a given process may be automated within the system, such as alarms, restrictions to data fields, required data fields, dialog box prompts for verification. Alternatively, they may be entirely independent external processes, such as subsequent chemical or physical analyses, or operator checks. Examples of controls that could be used to reduce risk are shown in Table 11.2.	Ⅰ
		16.3.2	All deliverables should be identified so that the controlled items subject to change management may be defined. These may include: • Configuration files (for configurable products, alarm, and process setpoints, etc.)	Ⅱ
		25.6.2	Specific types of testing should be considered, depending on the complexity and novelty of the system and the risk and supplier assessments of the system to be tested, including: • Normal Case testing (Positive Case or Capability testing) challenges the system's ability to do what it should do, including triggering significant alerts and error messages, according to specifications.	Ⅱ
		25.9.1.2	The following is an aide memoire only and does not replace the need to apply critical thinking and a risk-based approach to the scope and rigor of testing. It should be used simply as a reminder to help ensure appropriate test coverage of the installed system. Test coverage may include: • Power failure testing, especially • Alarms and error messages	Ⅱ
		29.3.2	Some of the factors to consider as part of risk assessment are: • For automated tools, for example, when considering performance monitoring, how are any alerts monitored and acted upon?	Ⅰ
		31.3	Development also requires consideration of human factors (e.g., usability challenges such as alert fatigue), cybersecurity, and legal liability. This requires transparency, and an understanding of the ability to reproduce outcomes, adequately interpret the results, and understand the relevance for how the models will be applied without bias.	Ⅰ
		35.4.3	System monitoring should consider the following: • System and process alarms and events	Ⅱ
		47.2.4	Other information such as trends and warnings recorded as an output of manufacturing are often used by production and quality personnel to determine long-term effects of operational tolerances and variances, but are not part of GxP production records unless directly related to GxP decision-making. Operational processing may have master data such as material specifications, process parameters, alert and alarm limits, or process step sequences controlled by several systems with functionality in the manufacturing domain (see Figure 47.1). Recipes may combine master data from one or more sources either by direct entry or by links to systems for the production environment for execution. Systems design and/or procedural controls should ensure that the version of all master data is known and controlled and can be demonstrated for any specific master recipe.	Ⅰ
		47.2.6	Data Processing Based on established CPPs and CQAs, key factors in processing data include verified rounding rules and other mathematical standards, calculation definitions, alerts, alarms, and specific events that may automatically create data or initiate other actions or further processing. Data audit trails and procedures for data review, (including audit trail reviews where relevant), is essential for process management, review and improvement, and investigations. Appropriate and effective security features, user management, and privilege management is essential.	Ⅰ
		47.4.1	The RBE method: • Filters EPR data presented to personnel - Includes human process/system interaction such as disposition and alarm processing - Reduces or eliminates reporting in-tolerance operational data, events, or alerts not required to support critical exceptions	Ⅰ
		47.4.2	RBE is enabled by the GAMP approach, where systems are appropriately specified and verified to ensure CPPs and overall systems operations are implemented correctly, and are appropriate to each process, process step, or system function. Following the GAMP approach should ensure the following: • All defined process or system alerts and alarms are generated when tolerances or other operating constraints are exceeded	Ⅰ
14	WHO-TRS 1033 Annex 4 Guideline on Data Integrity 2021 年	NA	NA	NA
15	PDA-No.80 Data Integrity Management System for Pharmaceutical Laboratories 2018 年	6.3.10.1	The transactional log (which may be referred to by other terms depending on the equipment vendor) and system error logs are online, instantaneous features that display pop-up messages about system functionality, user activity, and hardware-related issues or errors. The transactional log is neither an audit trail nor is it intended to be a replacement for or component of other audit trails. A transactional log generally provides some additional information related to soft-ware (e.g., missing vial, lost prime) or hardware malfunctions (e.g., HSS fault, lost connection) and can help in interpreting the audit trail. No one should have access or authority to manually change this log; however, the system can be configured to automatically purge the messages on a periodic basis to ensure efficient operation of the system process-ing memory. If the audit trail is never turned off, any deletion, modification, or copying of messages per-formed by the administrator will be recorded in validated audit trails (e.g., system audit trail). The Quality Unit should verify when a system or run has been interrupted due to a disconnection or power loss. The messages appearing in the log may come from the application software, third-party software, (e.g., Oracle database supporting system for chromatographic software) or other connected instruments (e.g., balance connected to HPLC) or equipment. Some chromatographic software packages offer this function-ality. The transactional logs are system-level messages, temporarily stored and often automatically purged by the system at time-based defined intervals; their utility is therefore time-sensitive. These transactional logs may prove beneficial for trending (e.g., trending of most frequent instrument or processing errors that require attention helps in troubleshooting) or investigational purposes (e.g., describing the cause of the failure) and companies may utilize this information accordingly. During software validation, messages will present as information, warning, or error according to listed categories (e.g., general, security). Critical messages and actions regarding data manipulation or data deletion that may appear in the transactional log must be captured in validated audit trails (e.g., system, result, sequence or sample, or method audit trails). Categorization of error messages having an impact on the software and product ideally would be incorporated during software development and validation by the vendor. Some errors with titles that sound critical (e.g., cable disconnected, connection lost, communication failure) may not be captured in a validated audit trail but recorded in a transactional log. It may be difficult to confirm that these types of messages are all caused by intentional interruptions or have any impact on product quality data. It is therefore important to have appropriate controls and procedures in place to ensure that true power outages be recorded, especially if a chromatographic run is affected. 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. For example, if a cable is disconnected from an HPLC to a LAC/E box, then the data will not be captured, and the transactional log will show a message as system interruption due to cable disconnection. Further dialogue between industry, health authorities, and vendors is needed to resolve how to address this evolving topic.	Ⅰ、Ⅱ、Ⅳ
		6.5.2	Common Deficiencies that May Lead to Data Compromise • Not investigating qualification errors or shortfalls according to nonconformance procedure	Ⅱ
		6.6.3	Since instrumental software may have some exceptional behavior, firms should document the communications with software vendors regarding clarification/remediation of error messages, warning messages, software bugs, and other issues that may be identified in audit trails, or other operations that need support from the vendor. These issues, communicated over the phone or via email, should be documented and will serve as a basis for change of procedures or initiation of new controls. Often vendor call centers or tech support groups allot a ticket number or tag number that can be referenced. In addition, there may be issues or restrictions in the software that a vendor would identify and communicate to all users through website notification or email communication. Firms should assess and document how those communications will be evaluated and how a determination is made regarding the effect on GMP operations. Recordings of audit trails and other critical data are recommended to be checked on a periodic basis to have better control and understanding of software issues. If any anomalies are observed they should be investigated immediately, and if they are suspected as software issues they should be communicated to the vendor for next steps of investigation.	Ⅱ
16	PIC/S 041-1-Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments 2021 年	9.1.5.2	In dealing with metadata, some metadata is critical in reconstruction of events, (e.g. user identification, times, critical process parameters, units of measure), and would be considered as 'relevant metadata' that should be fully captured and managed. However, non-critical meta-data such as system error logs or non-critical system checks may not require full capture and management where justified using risk management.	Ⅳ
17	APIC-Practical Risk-Based Guide for Managing Data Integrity 2022 年	7.4	System Audit Trail Review • Examples of areas to be included, but not limited to; o Significant errors, alerts or warnings as defined by company e.g., back up failures or issues	Ⅱ
18	ECA-GMP, GCP and GDP Data Governance and Data Integrity 2022 年	8.3.5	The SCADA technology (also called DCS Distributed Control System) is used to connect the PLCs with the MES (manufacturing execution system). SCADA systems allow staff or supervisors to change the settings and to monitor critical conditions like high temperature; lots of data is collected by them which can be monitored using the HM interfaces (part of the machine that handles the human–machine interaction). The operator interfaces enable monitoring and issuing of process commands, such as controller set point changes, are handled through the SCADA supervisory computer system. It consists of membrane switches, keypads and touchscreens. The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. SCADA systems are using combinations of radio and direct wired connections. The remote management or monitoring function of a SCADA system is often referred to as telemetry. The Data Lifecycle elements at this level are manual data capture, processing, transmission, saving and in some cases evaluation of data, alarms and events.	Ⅰ
		8.3.10	Data Categories • Process, alarm and event data	Ⅰ
		8.3.14	Data Lifecycle elements are one of the key elements to control data integrity in the manufacturing environment. Data Integrity strategies and risk mitigation have to apply at all phases of the data lifecycle. Sometimes not all parts of a data lifecycle elements are fitting to a particular component; therefore, adoption might be necessary. From a data point of view, it is important to demonstrate that all lifecycle components are covert [47]. 1. Data generation and capture automatically or manually The data lifecycle starts usually with generation and capturing of data no matter if this is automatically or manually generated data (e.g. continuous data flow from a sensor, alarm event or operator input during process). But the results regarding data integrity requirements a quite different. Date generation and automatic capture means data is generated by a sensor (e.g. temperature, humidity, pressure etc.) and captured in a computerized system. For this kind of generated data, no data integrity requirements should be applied. 2. Data processing & transmission Processing means that data is transformed according given rules or control logic, for example from one physical value to a meaningful information like temperature, humidity or pressure. Applying algorithms to "process" data might also part of this data lifecycle element and can result in creation of additional data (e.g., calculations, alarms, metadata etc.). Transmission to other systems in case components are connected to each other. 4. Data review, evaluation and reporting during production process Any decision made on reviewing, assessing or reporting data. This could be reviewing alarms by operator or any quality decision during manufacturing. For the review of data directly after entering by the operator the second person review by a peer is required for critical entries. Regardless of this first check an audit trail review must be performed before the release of the batch for further processing or quality control.	Ⅰ、Ⅱ
		8.3.18	Events & Alarms In the production process control center there are lots of alarms coming up during a working day. Each alarm represents an indication for an "out of control" situation or a deviation from normal process parameters. Very frequently it can be observed that operators are just acknowledging an alarm without taking further notice because they are aware that such alarm is coming up very frequently and that there is no critical situation occurring. The problem is that operators are getting too many alarms which is exceeding their capacity to deal with them. Sometimes they are losing the ability to deal with the "real important alarms". In these cases, it may be advisable to recheck the alarm limits.	Ⅱ
		8.10	GDP Critical Data Critical Process Parameters and Critical Alarms (such as Temperature Data) need to be defined with required actions within the GDP environment. These actions will also need to be recorded so that the alarm and event logs can be reviewed, where appropriate, to support critical decisions.	Ⅲ