Your Life Science
Compliance
Partner

Pharma 4.0

Data Integrity Checklist for Life Science

ellab

A Validation Readiness Checklist

In today's life science industry, data integrity is no longer just a compliance requirement, it's the backbone of digital trust. As Pharma 4.0 drives the shift toward connected, intelligent, and adaptive operations, data integrity practices must also evolve.

This checklist is designed to help you bridge traditional data integrity practices with the expectations of Validation 4.0. It supports accuracy, consistency, and security across your systems while ensuring readiness for regulatory inspections.

Formulated in line with FDA 21 CFR Part 11, EU GMP Annex 11, PIC/S guidance, and grounded in ISPE Pharma 4.0™ and Validation 4.0 principles, the checkpoints now emphasize not only compliance but also future-proofing your processes: Integrating digital tools, embedding ALCOA+ principles, and enabling continuous verification.

Whether you're just starting or refining a mature program, this checklist will guide you in:

- Embedding risk-based thinking into validation activities.
- Ensuring end-to-end traceability across digital platforms.
- Building inspection readiness by design, not as a one-off event.
- Connecting your compliance framework with the Pharma 4.0 vision of smarter, more resilient life sciences operations.

Nathan Roman

Purpose

This document is designed to provide you with the knowledge and tools needed to uphold data integrity practices, support quality assurance, and ensure regulatory compliance.

Whether you are new to these requirements or leading advanced programs, it will help you align your daily practices with ISPE Pharma 4.0™ and Validation 4.0 principles, and strengthen readiness for inspections in a connected world.

Scope

This checklist has been designed around essential ISPE governance and Validation 4.0 guidance, and structured in accordance with core GxP quality guidelines and standards, drawing from:

- ISPE Pharma 4.0™ and Validation 4.0 principles
- FDA 21 CFR Part 11
- EU GMP Annex 11
- PIC/S guidance

It emphasizes data capture, transfer, and protection within computerized systems while promoting a modern validation approach - one that integrates digital enablers, risk management (ICH Q9), and lifecycle quality oversight (ICH Q10).

By combining regulatory compliance with ISPE's Validation 4.0 framework, this checklist supports both robust inspection readiness and the strategic adoption of Pharma 4.0 technologies.

Instructions

For each aspect, you'll find checkpoint questions to verify readiness. Mark responses as Yes, No, or N/A, or use a checkmark where applicable.

As you progress, assess not only compliance but also alignment with Validation 4.0 expectations:

- Are processes digitally enabled and risk-based?
- Do systems support continuous verification rather than point-in-time reviews?
- Are people, processes, and technologies integrated to deliver audit readiness by design?

By applying the checklist through this lens, you ensure your data integrity framework is compliant today and resilient for the future of life sciences.

01.
Data Capture

Data capture is the foundation of both compliance and digital transformation. In a Validation 4.0 context, capture goes beyond accuracy and consistency - it also means ensuring metadata, audit trails, and connectivity are built in by design. Accurate and reliable capture ensures information is precise, consistent, and ready for further processing while enabling real-time visibility and life cycle traceability.

Sensor Installation and Validation	Completed
Is the correct model and serial number of the sensor installed, verified against inventory records?	
Is the sensor located at the designated monitoring point?	
Is the sensor securely fixed in place to prevent data variability?	

Calibration Verification	Completed
Does the calibration management SOP apply to the sensors used and is it approved?	
Are calibration certificates reviewed for validity and proper storage, and cross-checked with supplier records?	

01.Data Capture

Calibration Verification	Completed
Is there a current and valid calibration sticker on the sensor?	

Data Review and Validation	Completed
Is there an approved SOP for data review?	
Does the SOP specify responsibilities for data review and define acceptable data standards?	
Are procedures in place for handling data that does not meet the established criteria?	
Is the timestamp for each data entry synchronized with an approved time standard (e.g., NTP server)?	
Are measures in place to ensure that the timestamp cannot be altered by unauthorized users?	

Validation 4.0 Alignment	Completed
Is data collected directly into validated digital systems, eliminating manual transcription?	
Do sensors and monitoring devices integrate seamlessly with centralized platforms for real-time review?	
Are metadata (e.g., audit trails, calibration records) automatically captured alongside primary data?	

02.
Data Transfer

Effective data transfer processes are crucial for maintaining data integrity as data moves across systems and interfaces. Ensuring secure and accurate data transmission prevents data tampering and loss. This section provides insights into securing system interfaces, implementing encryption, and managing legacy data to maintain the integrity of your data during transfer.

System Interfaces and DataTransmission Security	Completed
Are data transfer interfaces secure and do they prevent data tampering?	
Are data encryption and checksums in place to ensure data integrity during transfer?	
Is there a protocol for maintaining system updates to ensure ongoing data accessibility?	
Is the retrieval and integrity of the backed-up data periodically reviewed, and has the backup and restore functionality been validated?	

02.Data Transfer

Legacy Data Management	Completed
Is there a comprehensive migration strategy in place for legacy data that includes assessment, conversion, and validation protocols to ensure data accuracy and usability in the new system despite initial compatibility challenges?	
Are old data formats compatible with new systems or is there a conversion process in place?	

Validation 4.0 Alignment	Completed
Are API-based or cloud-to-cloud transfers validated for integrity, with encryption and checksum controls in place?	
Are blockchain or immutable ledgers considered for critical data transfers?	
Does the system verify data authenticity continuously, not only at transfer points?	

03.
Data Protection

Under Validation 4.0, protection extends beyond basic access control to include cybersecurity resilience, predictive monitoring, and audit readiness by design. This section covers foundational controls while also encouraging forward-looking practices, such as AI-driven anomaly detection, living validation of systems, and integrated governance - that safeguard your data in a connected, continuous assurance model.

Access Control and Security Measures	Completed
Does the system require unique identification for each user?	
Are there protocols for user access levels and administrative task segregation?	
Are all data changes logged in a secure and comprehensive audit trail?	
Does the system lock-out the user after a defined number of unsuccessful login attempts?	
Does the system time-out after a defined period of user inactivity?	

03.Data Protection

Data Security and Integrity Protocols	Completed
Are electronic records produced in a non-editable format (.pdf) to ensure integrity?	
Are physical and IT security procedures routinely reviewed and updated?	
Is data backup performed regularly, with secure off-site storage solutions?	
Are security measures in place to protect the system's clock settings from unauthorized changes?	
Is there a regular audit to verify the synchronization and protection of timestamps?	
Does the system's audit trail include detailed information for each entry, such as the name of the user, the date and time of the event, the previous and current value of the data, and a reason for the change?	

Compliance and SOP Verification	Completed
Are all related SOPs, including those for change management and disaster recovery, current and inclusive of the monitoring system?	
Is there a regular review process for SOP compliance and system readiness?	

03.Data Protection

Validation 4.0 Alignment	Completed
Is anomaly detection or AI-based monitoring in place to flag unusual patterns in real time?	
Are cybersecurity controls (firewalls, intrusion detection, ransomware protection) validated as part of GMP assurance?	
Does the monitoring system support predictive maintenance to prevent data loss from equipment failure?	
Are validation reports integrated into a digital QMS for lifecycle traceability?	

By completing our Data Integrity Checklist and assessing and addressing these key points, you are proactively taking the necessary steps to preserve your organization's data and to ensure its accuracy.

Guaranteeing data integrity isn't just about compliance; it's about making informed decisions, upholding reliability, and mitigating risks. With Ellab's continuous monitoring solution your assets will be protected: Be inspection ready by design - continuous, digital, and resilient.

With Ellab's continuous monitoring and validation solutions, your data integrity framework evolves in step with Validation 4.0 expectations with our TrackView Pro solution for continuous monitoring.

Read more about our continuous monitoring solutions and find out how Ellab can help you with asset preservation.