SARTORIUS

Protecting Data Integrity—Evaluating Instruments in the Lab

Compliance with data integrity regulations begins with all data-generating instruments and extends throughout lab systems—evaluate your instruments and procedures with this checklist

What does data integrity mean for labs?

In the current age of digital transformation, improving operational efficiencies, streamlining workflows, and eliminating paper requires connected workflows with fully integrated equipment and systems. Maintaining data integrity forms a primary concern, particularly as auditors increasingly call for fully electronic data handling to improve security, contributing to the digitalization trend.

An expanding regulatory network affects an increasing number of labs as they connect to the highly regulated life science, biotech, pharmaceutical, and food industries, such as the fine chemical companies supplying pharmaceutical and biotech product pipelines. Non-compliance can result in shutdowns, product recalls, or delayed drug approvals, is costly, and places the organization's reputation at risk. The challenge of remaining compliant centers the need for improved data handling.

Beyond avoiding regulatory violations, data integrity measures that ensure the correct recording and handling of data increase workflow automation, minimizing errors common to manual or hybrid data entry, like transcription errors and data breaks. They increase reproducibility, efficiency, and time and cost savings, impacting important timelines like discovery time and time to market. Eliminating the need to repeat work because of inaccurate data or reporting helps organizations remain competitive.

Protecting data integrity

Compliance with FDA 21 Part 11 CFR guidelines, and the EU Annex 11 in Europe, requires supporting features for all electronic instruments in the lab within either native OEM software or third-party bridging software. Features supporting compliance include audit trails, access control with personalized user and role management, electronic signatures, data backup, and safe data transfer options for laboratory information management systems (LIMS), electronic lab notebooks (ELN), or other system integrations.

Most violations of FDA 21 Part 11 CFR guidelines, as indicated through FDA warning letters, arise from data integrity issues (79 percent). The majority of these involve access and role management, missing or incomplete audit trails, improper data handling, or failure to follow procedures. Personalized user accounts that limit access to functions specific to their role are required to meet user traceability and access control guidelines. A common violation arises from the use of a universal account, frequently with administrative permissions that allow users to change or manipulate data. Maintaining complete audit trails is critical and requires backups of all data generated, regardless of whether the data are correct. Complete traceability requires documentation of every instrument-related event, including adding new users or changing operational settings. Nonconformance to audits also frequently arises from transcription errors that occur when data are entered manually into LIMS and ELN.

Beginning with a top-down, systems view of operations helps ensure compliance is maintained across the lab through identifying gaps in data integrity measures and fostering a quality culture centered on compliance. Focusing primarily on specific instruments or software is likely to result in missing other key systems or problems where systems interface. The top-down approach ensures start-to-end traceability by first identifying all GxP-relevant

processes in the lab, then sub-processes, followed by individual activities with standalone systems and instruments. While analytical equipment is most often top-of-mind when considering data integrity measures, a detailed examination of processes typically identifies supporting lab equipment that must be included for complete traceability. Lab balances, for example, are foundational to data accuracy but frequently overlooked or only considered secondarily with the implementation of third-party software.

The value of instrument-based compliance support features

Some lab instruments come with native compliance support, negating the need for middleware, which reduces operating costs and simplifies qualification processes. The integration of data integrity features on an instrument like a lab balance improves data quality, helps bring control to the entire lab process, removes the ability to falsify process data or signatures, and reduces costs associated with rework. When acquiring new electronic lab equipment, considering the current and future needs of the lab throughout the digitalization process helps inform purchasing decisions.

A compliance-ready instrument needs to have technical control features, comprehensive audit trail features, and effective and compliant connection to LIMS, ELN, and other IT systems. FDA guidelines on data integrity require that data be complete, accurate, and consistent, and recommend following the ALCOA framework: attributable, legible, contemporaneously recorded, original or a true copy, and accurate. Instruments can be fully evaluating using the 21 CFR Part 11 compliance checklist provided below.

What does compliance support look like on an instrument?

The design elements required for onboard compliance support can be illustrated using the **Sartorius Cubis® II** lab balance. Designed using the ALCOA framework, the Cubis II with the QApp pharma package incorporates all technical control features required for adherence to CFR Part 21, Part 11 guidelines. A full walk-through of these features and how they support compliance follows.

Ensuring data are attributable requires inclusion of metadata, such as user ID, balance ID, sample and batch information, date and time, software version, etc. This relies on comprehensive user management and access control, which the Cubis II provides through local user management and centralized "single sign-on" user management options. Password and login security measures can be set in line with company policies. Final weighing reports including the relevant metadata can be printed or exported electronically with electronic signatures, which are tied to secure username and password combinations.

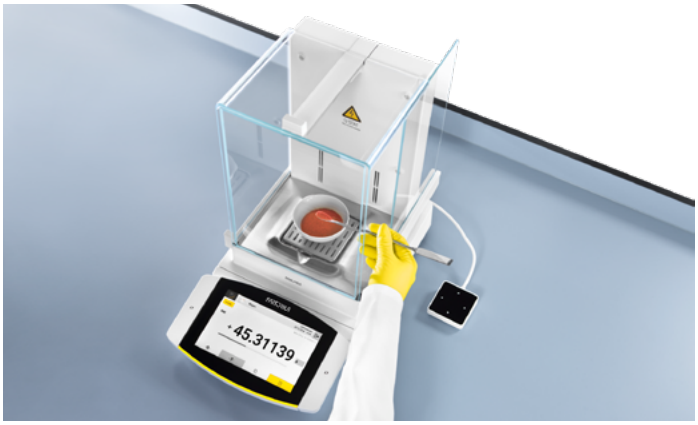
Full traceability is achieved with audit trails and advanced reporting. Audit trails consist of complete, tamper-protected, time-stamped data files that reflect all events relating to creation, modification, and deletion of records. The Cubis II is configured to deliver these data in filterable, exportable reports that are easy to read and understand. Additionally, it retains separate, immutable records of the last 150,000 datapoints in weighing data raw ("Alibi") memory.

Data must be recorded contemporaneously (at the time of generation) with accurate timestamps that are traceable to UTC. The Cubis II offers automatic time synchronization via network time protocol to ensure accuracy in metadata.

Origin, content, and meaning are preserved through file metadata and protected using a calculated MD5 checksum for each file by the Cubis II. This allows other IT systems, like LIMS, to verify authenticity and trustworthiness of data files.

Ensuring data are accurate and complete also requires proper documentation of all mistakes and corrections. The Cubis II allows users to mark incorrect datasets and add explanatory comments. Invalid datasets are clearly displayed using crossed out text accompanied by the correct dataset.

Full compliance requires additional procedural controls and long-term data storage systems in the lab. Data backup and archival are integral to protecting data in both the short and long term. Cubis II backups can be automatically scheduled and include audit trails, printouts, log files, Alibi memory, and configuration data. Archival can easily be performed by IT in a compliant manner, as records are readable without system-specific software.



Safe data transfer is an important capability for ensuring unbroken data integrity across systems. The Cubis II allows secure data transfer via multiple options, such as FTPS (secure file transfer protocol), SMB (Windows file server protocol), or external hard drive connection. It integrates easily and seamlessly with existing IT infrastructure, connecting securely to ELN, LIMS, and LDAP (Lightweight Directory Access Protocol) servers.

Full compliance heavily relies on human behavior, as well. The Cubis II further supports compliance through safety features like the "safe weighing" settings and through QApps (quality assurance project plans) that provide clear user guidance. This includes appropriate limits, tolerances, and best practices for reliable weighing results.

Compliance with data integrity guidelines requires correct recording, archival, and sharing of data. As digitalization transforms lab operations and regulations expand and evolve, it's increasingly important for labs to implement solutions that meet both current and future operational needs. Taking measures to protect data integrity helps organizations not only meet regulatory requirements but improve workflow efficiency and reduce costs.

How well do your lab instruments support data integrity compliance? Evaluate them using the checklist below.

For an example of the compliance checklist in action, **see how the Sartorius Cubis II stacks up.**

Instrument 21 CFR Part 11 Compliance Checklist

Overview			
Yes	No	NA	Is the system a Closed System, where system access is controlled by the persons who are responsible for the content of the electronic records that are on the system?
Yes	No	NA	Is the system an Open System, where system access is not controlled by the persons who are responsible for the content of the electronic records that are on the system? (e.g., a service provider controls and maintains access of the contents of the system, etc.)
Yes	No	NA	Does the system use an ID/ password combination?
Yes	No	NA	Does the system use tokens?
Yes	No	NA	Does the system use biometrics?
Subpart B – Electronic Records | 11.10 Controls for Closed Systems			
			11.10 (a)
Yes	No	NA	Is the application validated?
Yes	No	NA	Does the validation documentation show that Part 11 requirements have been met and are functioning correctly?
Yes	No	NA	Is it possible to discern invalid or altered records?
			11.10 (b)
Yes	No	NA	Is it possible to view the entire contents of electronic records?
Yes	No	NA	Is the system capable of producing accurate and complete copies of electronic records on paper?
Yes	No	NA	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?
			11.10 (c)
Yes	No	NA	Are records protected against intentional or accidental modification or deletion?
Yes	No	NA	Can all the archived data be accurately retrieved after system upgrades?
Yes	No	NA	Are the records readily retrievable throughput their retention period?
			11.10 (d)
Yes	No	NA	Is the system access limited to authorized individuals?

			11.10 (e)
Yes	No	NA	Is there a secure, computer generated, time stamp audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?
Yes	No	NA	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?
Yes	No	NA	Is an electronic record's audit trail retrievable throughout the record's retention period?
Yes	No	NA	Is the audit trail available for review and copying by the FDA?
Yes	No	NA	Can selected portions of the audit trail be viewed and printed or saved by inspectors?
			11.10 (f)
Yes	No	NA	If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?
			11.10 (g)
Yes	No	NA	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?
			11.10 (h)
Yes	No	NA	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data or instructions received?
			11.10 (i)
Yes	No	NA	Is there documental training, including on the job training for users, developers, IT support staff?
			11.10 (j)
Yes	No	NA	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signature?
			11.10 (k)
Yes	No	NA	Is the distribution of, access to, and use of systems operations and maintenance documentation controlled?
Yes	No	NA	Is access to "sensitive" systems documentation restricted e.g., net security documentation, system access documentation?
Yes	No	NA	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical organization?
Subpart B – Electronic Records 11.30 Controls for Open Systems			
Yes	No	NA	What controls ensure record authenticity, integrity, and confidentially?
Yes	No	NA	Are data encrypted?

Yes	No	NA	Are digital signatures used?
Subpart B – Electronic Records 11.50 Signature Manifestations			
Yes	No	NA	Do signed electronic records contain the following related information? The printed name of the signer The date and time of signing The meaning of the signing (such as create, approval, review, responsibility)
Yes	No	NA	Is the above information shown on displayed and printed copies of the electronic record?
Yes	No	NA	Are date and time stamps applied automatically (vs. being keyed in by the user)?
Yes	No	NA	Are date and time stamps derived in a consistent way in order to be able to reconstruct the sequence of events?
Yes	No	NA	Is the above information subject to the same controls as electronic records? (Audit trail, access control, etc.)
Subpart B – Electronic Records 11.70 Signature/Record Linking			
Yes	No	NA	Are changes to electronic signatures included in the audit trail?
Yes	No	NA	Do the printed name, date, time and electronic signature meaning appear in every human readable form of the electronic record (e.g. all screens and printed reports)?
Yes	No	NA	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied or otherwise transferred by ordinary means for the purpose of falsification?
Yes	No	NA	If handwritten signatures are executed to electronic records, are the handwritten signatures linked to the electronic record?
Yes	No	NA	If the electronic record is changed, is the signer prompted to re-sign (via either manual procedures (SOP) or technical means)?
Yes	No	NA	Are the electronic signatures linked (via technology, not procedures) to their corresponding electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?
Subpart C – Electronic Signatures 11.100 General Requirements			
			11.100 (a)
Yes	No	NA	Are electronic signatures unique to an individual?
Yes	No	NA	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else?
			11.100 (b)
Yes	No	NA	Is the identity of an individual verified before an electronic signature is allocated?
Yes	No	NA	Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?

			11.100 (c)
Yes	No	NA	Has certification of the intent to use electronic signatures been submitted to the agency in paper form with a traditional handwritten signature?
Yes	No	NA	Can additional certification or testimony be supplied to show that an electronic signature is the legally binding equivalent of the signer's handwritten signature?
Subpart C – Electronic Signatures 11.200 Electronic Signature Components and Controls			
			11.200 (a)
Yes	No	NA	Is the electronic signature made up of at least two components, such as an identification code and password, or an ID card and password?
Yes	No	NA	When several signings are made during a continuous session, is the password executed at each signing (Note: Both components must be executed at the first signing of a session)?
Yes	No	NA	If signings are not made in a continuous session, are both components of the electronic signature executed with each signing?
Yes	No	NA	Are non-biometric signatures only used by their genuine owners (e.g. by procedures or training reinforcing that non-biometric electronic signatures are not "loaned" to co-workers or supervisors for overrides)?
Yes	No	NA	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?
			11.200 (b)
Yes	No	NA	Are biometric electronic signatures designed to ensure that they can be used only their genuine-owners?
Subpart C – Electronic Signatures 11.300 Controls for Identification Codes/Passwords			
			11.300 (a)
Yes	No	NA	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?
Yes	No	NA	Are there procedures covering the initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information?
			11.300 (b)
Yes	No	NA	Are procedures in place to ensure that the validity of identification codes are periodically checked?
Yes	No	NA	Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alterations?
Yes	No	NA	Do passwords periodically expire and need to be revised?
Yes	No	NA	Is there a procedure for recalling identifications codes and passwords if a person leaves or is transferred?

Yes	No	NA	Is there a procedure for electronically disabling an identification code or a password if it potentially comprised or lost?
			11.300 (c)
Yes	No	NA	Is an SOP in place directing action to be taken to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices used to carry or generate electronic signature components?
Yes	No	NA	Does this SOP contain procedures for managing and controlling temporary or permanent token/card replacements?
			11.300 (d)
Yes	No	NA	Is there a procedure for detecting attempts of unauthorized use and for informing security?

Germany

Sartorius Lab Instruments GmbH & Co. KG
Otto-Brenner-Strasse 20
37079 Goettingen
Phone +49 551 308 0

USA

Sartorius Corporation
565 Johnson Avenue
Bohemia, NY 11716
Phone +1 631 254 4249
Toll-free +1 800 635 2906

For further contacts, visit
www.sartorius.com

Status: 02 | 2023