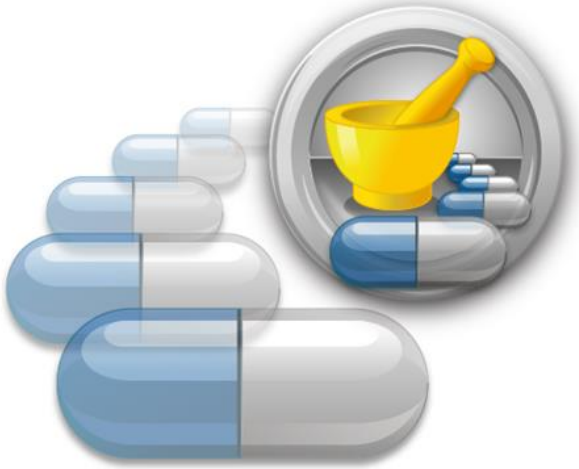
Implementation of

Data Integrity



FT PharmaSuite 10.02.00

How FT PharmaSuite® is helping regulated companies to achieve Data Integrity.

This document has been approved electronically via Rockwell's Document Management System [1].
This document contains information which is confidential and proprietary.

DIR: 10006111198/PUB Revision: 1.0

Copyright Notice

Trademark Notices

Disclaimer

Period of Validity

This document is valid for the release on the cover page – FT PharmaSuite 10.02.00.

Abbreviations

- RA: Rockwell Automation
- QMS: Quality Management System

Introduction

PharmaSuite

PharmaSuite® is a suite of software applications that is tailored to the needs of the Pharmaceutical and Biotech industry (in general: regulated companies). Special regulations are in place for these industries, and many of them also apply to software that is used during the course of production of a drug product. Therefore, the software has to be developed under consideration of the pertinent regulations and related requirements. In addition, appropriate validation of the deployed software system has to be performed before it can be used in the production environment.

PharmaSuite is developed under consideration of all pertinent regulations that are relevant for its use in the Pharmaceutical and Biotech industry. This is particularly true for the features of the software itself, but also for the process how the software is developed, which is based on a mature Quality Management System. Moreover, PharmaSuite includes extensive technical, functional, and quality documentation. With that, PharmaSuite meets all pre-requisites required for a successful deployment and validation at customer's site.

Data Integrity (DI)

What is data integrity? Here are some definitions taken from prominent sources:

“The extent to which all data are complete, consistent, and accurate throughout the data lifecycle.” – MHRA [2]

“The degree to which a collection of data is complete, consistent, and accurate.” – IEEE

“The assurance that information is unchanged from its source, and has not been accidentally or maliciously modified, altered or destroyed.” – NIST

“Data Integrity … is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence, and may ultimately undermine the quality of medicinal products.” – PIC/S [3]

“FDA expects that data be reliable and accurate … CGMP regulations and guidance allow for flexible and risk-based strategies to prevent and detect data integrity issues. Firms should implement meaningful and effective strategies to manage their data integrity risks based upon their process understanding and knowledge management of technologies and business models.” – FDA [4]

Setting the Stage

Across the life sciences industry, data integrity has always been essential to quality control – and regulatory compliance. But as the pharmaceutical supply chain has become more global and diffuse, maintaining complete, consistent and accurate data throughout the manufacturing lifecycle has become more complex.

Today's Challenges

Today, pharmaceutical companies typically rely on contract manufacturers for the active pharmaceutical ingredients (APIs) in their products. Yet an increasing number of cases citing poor quality data uncovered during API audits have sounded the alarms.

Violations range from poor records and deficient production process systems to escalating instances of "testing into compliance" or performing multiple laboratory tests until a sample passes. Although well-known for decades, the topic has received a lot of attention lately and is under the magnifying glass of inspectors globally since 2013.

Regulatory Expectations

The industry response? New data integrity guidance from regulatory agencies including the MHRA [2], PIC/S [3], FDA [4], and WHO [5] have been issued. The harmonization of these standards is an ongoing priority. As an example, the International Society of Pharmaceutical Engineering (ISPE) has compiled a guide to records and data integrity that seeks to provide an overview on and interpretation of existing regulations and guidance [6].

For pharmaceutical companies, data integrity violations can lead to production delays and drug shortages – and negatively impact public health and profitability. To help mitigate compliance issues, drug companies are requiring suppliers to apply more stringent quality controls – and expand their use of electronic records and technology.

Don't underestimate!

Why is data integrity so important? Today, most decisions are data-based, so the underlying information / data for decisions must be trustworthy. To put it straight:

> Quality and completeness of clinical, analytical, and scientific data is the basis of all important programmatic and daily risk / benefit decisions regarding selection and use of healthcare products.

As a consequence, erroneous or unreliable data may adversely impact product quality, and ultimately pose a risk to patient safety.

DI in a Nutshell

The following paragraphs will provide some examples for risks to, impact on, and findings related to data integrity. These lists are neither complete nor exhaustive.

Risks

What are the common risks to data integrity in an MES?

- Erroneous data due to human error during data entry
- Missing / incomplete raw data
- Uncontrolled changes without audit trail
- Invalid (e.g. inconsistent) data entries
- Inadequate archiving

Impact

In case the risks become an issue, what would be the impact?

- Misinterpretation of product quality, safety, or efficacy
- Adulteration of product
- Release of adulterated or quarantined product
- Misbranding of product
- Inability of product recall
- Incorrect product quality or patient safety decisions
- Incorrect submission to a regulatory agency

Findings

And what are the most popular findings of data integrity violations?

- Access control & security measures (shared user login, missing audit trail)
- No contemporaneous recording
- Data discrepancies are not being investigated
- Testing into compliance
- Critical (quality) data not adequately collected, retained, or reviewed
- Original data overwritten
- Fraud / data falsification

How does PharmaSuite Help?

In the past, paper-based production has been seen as the yardstick, but Manufacturing Execution Systems (MES) have become more and more popular for good reasons. Nowadays, electronic records are no longer seen as the problem, but as part of the solution:

> "Data integrity is underpinned by well-documented, validated GxP computerized systems, and the application of appropriate controls throughout both the system and data life cycles." [6]

So while an Electronic Batch Record (EBR) automates metadata collection and reduces human error, it does not intrinsically protect against undocumented or malicious changes to that data. But EBR as an integral part of MES definitely can help pharmaceutical suppliers maintain data integrity throughout their process.

Protecting your Data

How can this level of protection be achieved? A robust MES, like PharmaSuite, supports data integrity through a multitude of validation measures including:

- Access control for clients (and servers).
- Controlled administration of user rights and access privileges.
- Automatic recording of changes to electronic records ("audit trail").
- Consistency checks during recipe design and execution.
- Status management of recipes, workflow, and equipment.
- Automation layer integration with standardized interfaces for automated data acquisition.
- Weigh and dispense embedded in EBR.
- Fully integrated exception management in EBR.
- Testing and monitoring interfaces with other systems.

This document describes several of these aspects that have been considered from the beginning in design, specification, implementation, and testing of PharmaSuite, in more detail.

A Sound Baseline

In addition to individual measures that help mitigate risks and protect your data, PharmaSuite is developed following a proven methodology that includes current SW engineering techniques and quality assurance measures like

- Modular design
- Scalable architecture
- Tracking / recording of all activities (incl. extensive documentation)
- Code and design reviews
- Continuous integration
- Risk-based testing (incl. automated tests)
- Risk, safety, and security assessments

Simply put, a validated system – combined with a high level of integration – promotes a high level of data integrity.

Integration Levels

To help ensure a single data source and consistent workflows across the enterprise, an MES can be integrated, e.g. with the automation layer, with Laboratory Information Management (LIMS), – and with ERP systems.

Further Reading

As data integrity is not a new concept, we recommend to take a look at PharmaSuite's implementation of FDA's 21 CFR Part 11 ([7], [8]) and EMA's Annex 11 ([9], [10]), too. Both documents shed more light on additional compliance aspects of PharmaSuite and describe some of the topics highlighted here in more detail.

Non-technical DI Aspects

As outlined in ISPE's guide to records and data integrity [6], data integrity includes many aspects like

- Organizational culture
- Procedural controls
- Human factors
- Critical thinking
- Data governance
- System maturity
- …

These aspects cannot be addressed by a computerized system (or only to a very small extent), but need to be covered by other means. Consequently, these aspects are out of scope for the considerations in this document.

And please keep in mind:

- If an operator enters a wrong value, the application cannot detect it (while it can detect violations of defined limits, it cannot verify the entered data in general).
- No application can distinguish between a mistake and a fraudulent activity.

Examples of DI Supported by PharmaSuite

PharmaSuite supports data integrity by various validation measures, including but not limited to:

- Testing and monitoring of server communication
- Consistency checks
- Status management
- Automatic recording of changes
- Exception management
- Configurable system rights

These topics will be outlined in the following sections.

Testing and Monitoring of Server Communication

Interfaces of PharmaSuite are specified and verified like other features. As the PharmaSuite clients interact with numerous servers (depending on the configuration), a server heartbeat check has been implemented and is monitored through a "watchdog" process. This includes the following aspects:

- Availability check at application start
- Continuous (cyclic) verification of server availability
- "Server unavailable" message to operator

However, even in case of a server being unavailable (or unreachable), PharmaSuite's robust architecture helps to continue working with a client without server connection for some time, as parts of a recipe or workflow can be executed locally.

Consistency Checks

Consistency and validation checks have been implemented across PharmaSuite, from recipe authoring to execution. As recipes and workflows for production can become quite large and complex, the Recipe & Workflow Designer provides far more than 100 checks when configuring a recipe, for example:

- Correct usage of recipe elements
- Type and number of parameters
- Conflicts between parameters
- Links and transitions between recipe elements

When running these checks and presenting the results to the recipe author, PharmaSuite clearly distinguishes between errors, warnings, and information messages. All messages are clearly displayed in a separate window that supports easy navigation (via mouse click), thereby allowing rapid correction of any detected flaw. Recipes or workflows that (still) contain errors cannot be promoted to be *Valid*, thus preventing their execution in the Production Execution Client (PEC). Additional measures like re-use of approved recipe elements with individual blocking (and locking) of parameters and structures further helps to make recipe authoring as smooth as possible.

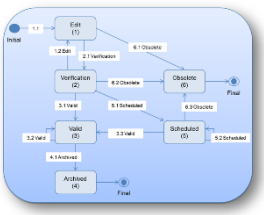
Finally, recipes and workflows will be verified and approved, ready for execution.

Similar to the authoring stage, data evaluation must be part of Electronic Batch Recording (EBR) at execution time, including checks like

- Is the operator authorized to execute the action?
- Does the identified batch meet all requirements, e.g. quality status, expiry date?
- Does the identified equipment meet all requirements, e.g. cleaning status, capabilities?
- Are all entered or acquired values within warning and alarm limits?
- Are all subsystems available?

Needless to mention that all actions (incl. operator and timestamp) are automatically recorded and are immediately available for review. But although careful preparation helps, operators may face unexpected situations during recipe execution. In these situations, PharmaSuite helps by providing extensive exception handling capabilities (automatic and manual) and a robust system architecture that allows seamless continuation of execution at a later point of time (when the system has recovered).

Status Management



PharmaSuite provides many different statuses for all relevant objects like recipes, workflows, equipment, and exceptions. Prominent examples are recipes that must be *Valid* before they are available for execution or equipment that comes with a cleaning, test, or calibration status that is verified at time of identification.

Most of these statuses and transitions are configurable and typically executing a transition (e.g. approving a recipe by changing its status from *Verification* to *Valid*) requires an authorized user (and may be additionally secured by requesting an electronic signature).

Automatic Recording of Changes

Changes, events, and exceptions are automatically logged for almost every action in PharmaSuite in various variations:

“Classic” Audit Trail

Any changes to master data objects like material are recorded following 21 CFR Part 11 requirements (who changed what when and why?) [7].

Transaction History

For more “volatile” objects like batches, handling units, and equipment, especially for all inventory-related data, PharmaSuite keeps a transaction history (when was a batch consumed and in which orders has it been used?).

Change History and Logbook

For equipment such as rooms, scales, and containers, PharmaSuite provides a complete change history for all master data. Furthermore, a logbook can be configured to provide meaningful details of its usage during the entire life cycle.

Electronic Batch Record (Batch Protocol)

All recorded data as well as subsequent changes to electronic records (GMP-compliant corrections) in the context of recipe execution (e.g. post-completion actions) are part of the batch record / batch report.

Exception Management

PharmaSuite features a sophisticated exception management that is fully integrated into EBR. It helps to easily record and review any violation of expected values or resources (e.g., limit violation, violation of material or equipment requirements) and subsequent changes to electronic records by providing the following functions:

- Configuration of risk level, additional descriptions, and signature privileges during recipe authoring.
- Consistent handling and recording of exceptions throughout the execution.
- Canceled exceptions are still recorded in the Batch Record
- Real-time availability for review through the Exception Dashboard.
- Control of user authorization during review and closure of exceptions.

Configurable System Rights

PharmaSuite allows to manage and assign users, user groups, and access privileges (user rights incl. electronic signature) on multiple levels. Here are few examples:

- *Application*
  User A may access the master data management client (PMC), but not the execution client (PEC).
- *Use Case / workflow*
  User B may use the inventory-related workflows in PEC (incoming and outgoing goods, relocation …), but not Weigh & Dispense.
- *Action*
  User C can enter data in the context of the execution, but cannot sign off exceptions.

EMA, Annex 11, and Data Integrity

According to [11], this is the current[1] mapping of ALCOA aspects to Annex 11 paragraphs:

		Annex 11
A	Attributable (data can be assigned to the individual performing the task)	[2], [12.4], [15]
L	Legible (data can be read by eye or electronically and retained in a permanent format)	[7.1], [9], [10], [17]
C	Contemporaneous (data is created at the time the activity is performed)	[12.4], [14]
O	Original (data is in the same format as it was initially generated, or as a 'verified copy', which retains content and meaning)	[8.2], [9]
A	Accurate (data is true / reflective of the activity or measurement performed)	[Paragraph "Principles"], [5], [6], [10], [11]

[1] As of August 2016

References

[1] Rockwell Automation Document Management System (DMS), , basic functionality included in central SAP

[2] MHRA GxP Data Integrity Definitions and Guidance for Industry (Draft, Jul. 2016)

[3] PIC/S PI 041-1 "Good Practices for Data Management and Integrity in regulated GMP/GDP environments“ (Draft, Aug. 2016)

[4] FDA – Data Integrity and Compliance with CGMP (Guidance for Industry, Draft, Apr. 2016)

[5] WHO Annex 5 Guidance on Good Data and Record Management Practices (May 2016)

[6] ISPE Records and Data Integrity Guide (Apr. 2017)

[7] 21 CFR Part 11 – Electronic Records; Electronic Signatures; Final Rule; Part II; Department of Health and Human Services, FDA; March 20, 1997, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11

[8] PharmaSuite 10.02.00 – Implementation of 21 CFR Part 11, DIR 10006111194/PUB

[9] EudraLex Volume 4 –Medicinal Products for Human and Veterinary Use: Good Manufacturing Practice; European Commission; Annex 11: Computerised Systems; Jun. 2011, http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf

[10] PharmaSuite 10.02.00 – Implementation of Annex 11, DIR 10006111196/PUB

[11] EMA, Questions and answers: Good manufacturing practice; Data integrity (http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp&mid=WC0b01ac05800296ca#section16); Question #13

[12] PharmaSuite 10.01.00 – Implementation of Data Integrity, DIR 10005692387/PUB

Revision History & Approvals

Revision History

The following table describes the history of this document. The dates of each version are captured in the Document Management System [1].

Version	Author	Description
1.0	Eva Mueller	Initial document creation, based on [12].

Approvals

Approvals are captured electronically on the organization's Document Management System [1]. The required approvers of this document include the following:

Name	Role
Andreas Grossmann	Product Manager
Steffen Landes	Development Manager
Eva Mueller	Test Manager