Macedonian pharmaceutical bulletin, **68** (2) 77 - 96 (2022)
ISSN: 1857-8969
DOI: 10.33320/maced.pharm.bull.2022.68.02.009
Professional paper

Risk based approach on data integrity aspects of configuring computerized system in GMP laboratory

Marina Mandzukovska Micevska[1*], Gjorgi Petrusevski[1], Rumenka Petkovska[2]

[1]*Alkaloid AD-Skopje, Blvd. Aleksandar Makedonski 12, 1000 Skopje, Republic of North Macedonia*
[2]*Faculty of Pharmacy, Ss. Cyril and Methodius University in Skopje, Mother Theresa St. 47, 1000 Skopje, Republic of North Macedonia*

Received: November 2022; Accepted: December 2022

Abstract

Implementing computerized system in QC laboratory requires detailed planning of the configuration considering that data integrity must be maintained through the whole life-cycle of the computerized systems. Identifying critical data integrity issues and assessing the possible risk to the whole process enables establishing suitable measures for assuring data integrity. Those measures are implemented in configuration of the system, which increased the security of the data and established controlled workflow. Creating methods which perform calculations reduces the time necessary for calculations and their validation, and verification for suitable use enables security and correctness of the obtained results. This makes the process of analysis more effective by reducing the possibility of human error and allowing for more detail via automation. At the end, adequate and carefully configured computerized system followed by proper validation, increases the data integrity, facilitates the analysis and reduces the time of review.

Key words: computerized system, data integrity, risk assessment

Introduction

The use of computerized systems is gaining momentum in pharmaceutical industry. Since the regulatory requirements are more and more strict about satisfying data integrity demands, computerized system facilitate the data management and compliance with the regulatory requirements. Besides that, use of computerized system enables saving time which is essential in environments when the results are expected to be fast and accurate. Also, computerized systems replace manual processes which decrease the possibility of human error. But still, computerized systems are created and controlled by humans, and the possibility of error still exists. Thereby, adequate configuration, by respecting the rules of GMP is essential for proper functioning of the computerized system and assuring data integrity. Also, in regulated environments it is necessary to implement appropriate processes to ensure the accurate management of the computerized system. The responsibility to the end – user is to assure that system used is in accordance with relevant regulations.

Background

Regulatory background

Since the begging of the use of the computerized systems until now, most of the regulatory agencies have issued guidelines which address this subject.

*email: mmandzukovska@alklaoid.com.mk

The regulatory requirements of the European Union are consisted in EudraLex, where the matter of computerized systems is contained in Volume 4, especially in chapter 4, Annex 11 and Annex 15. Chapter 4 is named Documentation and consists the key principles of good documentation practice including electronic records which is important for GMP aspects of computerized systems. Annex 11, which is named Computerized Systems and applies to all forms of computerized systems used as a part of GMP regulated activities. Annex 15 describes the main principles of qualification and validation which apply to the computerized systems too (EudraLex, 2011a; EudraLex 2011b; EudraLex, 2015).

Another European guideline about computerized system is published from OMCL network, where the main principles of validation of computerized systems are explained. OMCL have issued two additional annexes where the validation of excel spreadsheets and validation of complex computerized systems is detailed (OMCL, 2018a; OMCL, 2018b).

The regulations of the USA are consisted in Code of Federal regulation, which title 21 is reserved for rules of the FDA. The GMP regulations which refer to the computerized systems are stated in 21 CFR 211 – cGMP. 21 CFR 11 is very important part, where are set forth the regulations about electronic records and electronic signatures which are used in the computerized systems. The need for validation of computerized systems is stated in 21 CFR part 820 which address quality system regulation (21 CFR part 211; 21 CFR part 11; 21 CFR part 820).

Additionally, the subject of computerized systems is elaborated by PIC/S – Pharmaceutical Inspection Co-operation Scheme, which guide to good manufacturing practice part II contains chapter about the general GMP requirements of the computerized systems. Also Annex 11 and Annex 15 have the similar requirements about the computerized systems as appropriate annexes of EudraLex (PIC/S, 2022).

In WHO publication Specification for pharmaceutical preparations, Annex 4 – Guideline on data integrity, the chapter 11 highlights some specific GMP aspects relating to the use of computerized systems (WHO, 2021).

AGIT which stands for Swiss working group on information technology has issued several guidelines on computerized system. There are separate guidelines about acquisition and processing of electronic raw data, archiving of raw data, validation of spreadsheets and validation of computerized systems (Agit, 2018).

ICH refers to the computerized systems in the guideline Q7 good manufacturing practice for Active pharmaceutical ingredient, where chapter 5.4 states the main GMP requirements about computerized systems (ICH, 2000).

On the other hand, GAMP has several good practice guides for computerized systems, which help to narrow interpretation of regulatory standards for improved compliance and quality (GAMP, 2017; GAMP, 2022).

A computerized system can be defined as a set of software and hardware components which together fulfil certain functionalities, which are performed by trained personnel, together with the network components, the controlled functions and associated documentation (Agit, 2018; EudraLex 2011b; OMCL, 2018a).

LabX software

LabX software is an integrated instrument data system that links multiple instruments in a single analytical workflow. The data collected into the LabX system are generated from the connected instruments. LabX software is applied in QC laboratory, which is GMP regulated environment, and its' principal use is connection of analytical balances into a centralized software. Balances enable measuring of standards and samples, and the measured values are used in calculations in the most specification parameters and as such it is critical that the obtained data are reliable.

The system produces data which is used to release components or materials and the system generates information in an electronic form that is required by regulatory agencies (Chandra, 2021). Since it is completely inappropriate for the weighing data to be gathered by observation, an analytical balance must at the very least have a printer attached. Paper printouts from small instruments like balances provide a high regulatory risk and hinder business efficiency because a printer has the potential to be compromised. Additionally, the analytical balance manual process flow is time consuming, entirely manual, sensitive to transcribing errors, subject to errors in calculations made with a calculator, and error-prone when data is manually entered into a computer system. However, post-run data fabrication can be challenging to spot, particularly when spreadsheets rather than a secure instrument data system are used to produce reportable results. Therefore, data generated from balances are initial step in every analysis and any error can affect the whole process which can lead to its repetition and its cancelation. Connecting the balances to a centralized software increases the speed of analysis and the speed of review, assures contemporaneous recording of data and provides elimination of paper.

LabX performs calculations and automatically which enables minimizing mistakes and calculation errors. All weighing data, including metadata, are automatically stored in a centralized database at the time of creation. LabX is a complex software that can be configured to the specific needs of the user's business process. As such it falls into the GAMP 5 Category 4 – Configured products. Configuring of the software, setting signature and account policies must be performed carefully, considering regulatory demands and ensuring that the results generated from the system follow the ALCOA+ principle. There is a general misconception that data integrity failures only result from acts of deliberate fraud. Yet in the collective experience, the majority of issues relate to bad practice,

poor organizational behavior and weak systems, which create opportunities for data to be manipulated (Churchward, 2015).

Recent regulatory guidance's, highlight the importance of implementation of risk-based approaches to ensure data integrity. For example, the FDA guidance explicitly notes that CGMP regulations and guidance allow for "flexible and risk-based strategies" to prevent and detect failures to ensure data integrity (FDA, 2018). Similarly, the MHRA guidance describes a risk-based approach to data management that includes the assessment of "data risk, criticality, and lifecycle" (MHRA, 2018). According to EudraLex Annex 11, risk management should be applied through the lifecycle of the computerized system taking into account patient safety, data integrity and product quality (EudraLex, 2011b). The purpose of this paper is to demonstrate how LabX computerized system in configured in GMP environment, based on a risk assessment, by minimizing data integrity deficiencies to the extent that it does not affect the quality of the generated data.

Risk assessment

The main purpose of the risk assessment is to identify the aspects of configuration of computerized system with impact on patient safety, product quality and data integrity and specifically to identify any areas of high risk requiring additional controls. The risk assessment was performed with FMEA (Failure Mode Effects Analysis) method. FMEA provides an organized, critical analysis of potential failure modes of the system being defined and identifies associated causes (ICH, 2005). It uses occurrence and detection probabilities in conjunction with a severity criterion to develop a risk priority number (RPN) for ranking corrective action considerations. RPN (Risk Priority Number) has been calculated on the basis of multiplication of the following indicators: severity (Table 1), detection (Table 2) and probability (Table 3). Categorization of the risk is presented in Table 4. The data integrity risk and the influence of the mitigating controls with configuration of the LabX software is assessed in Table 5.

Table 1. Factor of severity of damage

Severity of damage	Numerical Value
No excpected impact/damage wihout or with insignificant consequences for the patient/user/process	1
Impact can be expected/damage quickly dissapears without causing irreversible or long-term effect	2
Excpected impact/damage with considerablw implucations that need some time to disappear/ develomepent damage requires intensice and/or prolonged treatement	3
Geat influence (unauthoized)/ damage which is irreversible and can;t be repaired/ can pose a trea to life and/or public health/process/work of the company	4

Table 2. Factor coefficient of frequency of occurrence of the risk

Frequency of occurence	Numerical Value
The risk probably does not arise	1
The risk may occur once in year	2
It occurs more often, on six months	3
It occurs often to very often, every months	4

Table 3. Coefficient of detection

Frequency of occurence	Numerical Value
Detection of the risk is possible at the begginig of the process	1
Detection of the risk may be possible during the process	2
Detection of the risk can be possible at the end ov the process	3
Risk detektion is not possible	4

Table 4. Risk categorization

Frequency of occurence	RPN
LOW (Routine rocedure, monitoring, it is not necessaary to take measure	1-4
MEDIUM (Long term actions required)	5-16
HIGH (Action plan required)	17-32
CRITICAL (Immediate actions performed)	55-64

Table 5. Data Integrity Risk Assessment

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
Data acquired from the instruments must be checked for accuracy	Incorrect data is transferred to LabX/	Production of incorrect results	3/2/1	6	Check of data transfer in installation configuration	1/1/1	1
The system must be accessible to authorized users only	User can access system without being authorized.	Data might be falsified.	3/1/3	9	The user management is configured with password protection.	2/1/3	6
Attempts for unauthorized use must be detected	Lockout policy does not apply and further attempts are not blocked	The system does not block the user, no notification is sent to the administrator in order to reset the user account	3/2/2	12	the rules set for Active Directory are applied for LabX. Once the authentication is blocked from Active Directory this applies for LabX	1/1/1	1
It must be possible to add / retire users	Users cannot be added or retired.	System cannot be used as required	2/1/2	4	Users can be added and deleted. A user name that is associated with an account will no longer be accessible or usable, if the account is deleted.	1/1/1	1
Each user must have individual account	To be generated two users with same credentials instead of one unique	Two people can log into the system with same credentials	3/2/2	12	Labx is integrated with active directory and the system enforces that each individual user must have a unique user identity	1/1/1	1

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
It must be possible to manage users centrally	Users cannot be managed centrally	System cannot be used as required.	3/1/2	6	With the aid of Active Directory, the administrator can grant and limit access to users of the network	2/1/2	4
Password should be obscured when entered	Passwords when entered are not obscured and they are visible	Unauthorized person can gain access to the system	3/3/1	6	Since password management are imported from Windows environment, entering password is obscured	2/2/1	4
The software must have possibilities for creating user accounts	The system does not allow new user creation	The new user cannot access the system	2/2/3	12	Users can be added, changed, deleted or temporarily disabled	1/1/1	3
The software must create unique user identities within the database. A second account with the same name cannot be created	Software allows creation with same credentials as existing user	There is a risk of unauthorized access to the system.	2/2/3	12	Once an account is created, it is not possible to change the user name associated with it. It is not possible to create two accounts with the same user name	1/1/2	2
The system must have various user – defined access control levels	It might not be possible to define different Roles and Access Groups s to properly reflect different processes.	User could have more privileges than required. This could lead to deletion or falsification of data by mistake.	2/2/2	6	User types are defined and each user type has individual access privileges.	1/1/2	2
Clear assignment of users, roles and privileges should be defined	The users are not grouped in roles, and they have not clearly assigned privileges	Inadequate control and protection of data	3/2/2	12	The roles that are used in the system are defined. Thera is no user outside the defined role. Each role has clearly defined rights and privileges	2/1/3	6

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
Full use should be made of access controls to ensure that people have access only to functionality that is appropriate to their job role	Access controls are not defined	Inadequate control and protection of data	3/2/2	12	The roles are created according to the appropriate job role of the users, and privileges of the roles are granted accordingly	2/1/2	4
It must be possible to limit user management to a central administrator role	Other users gain administrator privileges	Data access compromised	3/2/2	18	The role IT administrator is created with granted administrator rights. Other roles have denied possibilities to edit administrator settings.	2/1/1	2
The users with administrator privileges must not be included in other groups	Users with administrator rights are included in roles with direct interest of the data	Possibility of unauthorized changes of data	3/2/3	18	The group IT administrator is restricted to minimum people possible, and those users are not included in other roles	2/1/1	2
System Administrator rights must not be assigned to individuals with a direct interest in the data.	Users have administrator rights	Uncontrolled change of the access rights and uncontrolled change of the data	3/2/3	18	Through user management the groups with direct interest in the data do not have granted administrator rights	2/1/1	2
Personnel with appropriate knowledge and experience should be responsible for reviewing and checking the data	There is no defined procedure for checking the data	The data are not checked and incorrect results are issued	3/2/3	18	Roles reviewer and approver are created which are experienced users and have appropriate granted privilege. In signing procedures, the signature of roles reviewer and approver are required for the approval of the result sets.	2/1/2	4

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
Appropriate controls must be established that changes to GMP records can be made by authorized personnel	There are not established controls over change to GMP records	Any user can make changes to GMP records	3/2/3	18	The privileges of creating methods and report templates are granted only to the user group senior analyst. Methods and report templates can be used after they are reviewed and approved and have status released.	2/1/1	2
Results cannot be deleted	Results can be deleted	Loss of data and possibility of falsification of results	3/2/3	18	The software does not enable deleting of the results and such privilege cannot be granted to any user.	1/1/1	1
It must be possible to enter comments when adding, deleting, changing or modifying objects.	Comments cannot be added.	Full traceability is not ensured.	2/1/3	6	The required step of entering a comment is included in signature policies, when reviewing or approving the objects	2/1/2	4
It must be possible to define processes including process steps requiring electronic signatures	Signing steps are not active	Data cannot be signed by approver and reviewer	3/1/2	6	Each individual account has electronic signatures privileges. Signing procedures are defined for the approval of versioned object.	1/1/1	1

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
Controls must be established over deleting of methods, weights, report templates	Granted privileges are exceeded and a user can delete data	Data will be deleted	3/23	18	In user management the privilege of deleting methods, weights and report templates is granted to the role IT administrator. In signature policies it is defined that the deletion of this objects is possible after approval of reviewer and approver and with mandatory comment	2/1/2	4
For review and approval e-signatures must be utilized	No electronic signatures can be used.	Required signatures could not be managed by the system and the data would not be automatically protected against change.	3/1/2	6	Signing procedures are defined for the approval of versioned object, and the option for two signatures of reviewer and approver is activated, and signing procedures require password.	1/1/1	1
Electronic signatures must be unique to an individual	Password is corrupted, no electronic signing is possible	The electronic signature is disabled	3/2/3	18	Password policy is according security settings in Active directory. All electronic signatures are password protected	2/1/1	2
The system must identify whether a record has been modified after application of the electronic signature	The data can be changed after electronic signature	The obtained data are not reliable	2/2/3	18	Any changes made on a record after signing are recorded in Audit Trail.	2/1/3	6

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
It must be possible to revoke approval	It is not possible to remove an electronic signature.	Issues identified in the Review / Approval process could not be corrected.	2/1/3	6	In access control privileges, the possibility for revoking the approval is granted to the roles reviewer and approver.	2/1/2	4
For all e-signatures: are user ID, date and time and reason present	The e-signatures are not connected to the appropriate user and the time of action	The data re not contemporaneous	3/2/3	18	E-signatures are shown in result sets of the current task with information about the user ID, date and time and appropriate comment. The report templates are configured to show electronic signatures, date and time of the review and approval and appropriate comments	2/1/3	6
Audit Trials have to be available for all parts, operations, processes and data of the system	A process is not logged in Audit Trail	Full traceability is not ensured	3/2/3	18	The function Audit Trail records all important activities to provide documentary evidence of the sequence of activities that have affected at any time a specific operation	1/1/3	3
Audit trial entries must include operator identity and must be date stamped	A data is not logged in Audit Trail	Full traceability is not ensured	3/2/3	18	Records in Audit Trail log contains operator ID and time and date of the event.	1/1/3	3

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
It must be possible to view, filter and print audit trials	Search function is not working	Specific data logs cannot be easily found	2/1/3	6	Audit Trail can be searched by different search criteria like task number, user name, instrument number method name. Audit trails can be exported and printed	1/1/3	3
Audit trail must include reason for changing of the data	The comments are not displayed in audit trail	Full traceability is not ensured	2/1/3	6	Comments are enabled for Audit Trail	1/1/3	3
Any type of failure/error of instruments should be recorded	A data is not logged in Audit Trail	Full traceability is not ensured	3/2/1	6	In such a case in Audit Trail there will be log “Instrument cannot be reached	1/1/1	1
All users must be unable to modify audit trial	Users can make modifications to audit trail	Audit trail can be changed deleted and data can be falsified	4/2/3	24	No potential failure possible as this is not adjustable system function. In access privileges there is no privilege available for any user to modify audit trail.	1/1/3	3
The results are reportable as in specification	There is no possibility of adjusting the decimal and measuring units of the results	Inadequate interpreting of the result	2/1/3	6	In the method function result, in the appropriate fields, the decimal and measuring units according to specification are entered	2/1/2	4
The results must be easily accessible	There is no possibility to search the results	The specific result is difficult to be found in the software	2/1/3	6	The results can be accessed in the folder result set, where can be searched by different search criteria like task number, method name, user name.	2/1/2	4

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
The software must enable calculating of the results	The software does not have the option for calculating the results	The results are calculated in a spreadsheet and entered manually which increases the possibility of error	3/1/2	6	All methods that are created to calculate results, have the function result which allows entering a formula which does calculations. Calculations are performed by using the results from the measurements	2/1/1	2
The results must be recorded at the time of creation	The time traveling is enabled	Possibility of falsification of the data	4/2/3	24	LabX server is installed on the network and time is synchronized form a trusted time source. Access to the clock is restricted to the IT personnel only.	1/1/3	3
There should be a defined procedure for naming of the methods	There are no defined criteria for naming the methods	The methods are not organized and the methods cannot be connected to the appropriate results	2/2/2	6	The naming of the method is according to the defined naming convention. In the part ID the department and the type of the instrument is entered, and the name of the method contains the type of action or specification parameter which is performed by the method.	1/1/2	2
The traceability of the method must be ensured	There is no traceability of the methods	Changes of the used method are not visible.	2/2/2	6	Every time a method is changed, a new version is created and the old version is stored in the system. Each user group has the privilege to view the previous versions of the methods	1/1/1	1

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
There must be an adequate control over the use of the methods	The use of the methods is not controlled	Anyone can create and use any method which can lead to incorrect results	3/2/2	18	Creating of the method is assigned as a privilege to the group senior analyst. In the signature policies the signatures of reviewer and approver are required for releasing of the method. In the access privileges the analyst have denied the right to use unapproved methods.	2/1/3	6
Results must be displayed in printable reports	Result cannot be printed	Results cannot be displayed for suitable format	2/2/2	8	Results are displayed in printable format, by choosing appropriate report template. For each method there is different report template.	1/1/1	1
The result includes the appropriate metadata	There is no possibility to enter the metadata of the result	The data are not complete	2/2/3	12	In every method a method function text in entered where is mandatory entering the data (name, batch number, potency) about the standard or the sample measured. Also, in the method function sample ID, the field of entering sample identification is set to be mandatory	2/1/2	1

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
The results must include sufficient metadata sufficient to support investigation and reconstruction of the entire data history	There is not enough metadata	The results are no attributable	3/23	18	When opening a task in the result set information about the measured sample, time of measurement, who performed the analysis, the name of the reviewer and approver, appropriate time stamps as well as the raw data of every step of performing the method is included. Also, results display the name of the method and the name of the instrument used	2/1/2	4
Calculations performed by the software must be validated	The calculations are not validated	The results are inaccurate	4/2/3	24	There is a defined procedure for validation of calculations. All calculations are verified by the system independent from the software. Every step of the validation is documented and approved by responsible persons.	2/1/2	4
Reports must be protected from unauthorized change	Any user can create and change the reports	The created reports are not reliable	2/2/3	18	In the access rights the privilege of creating the report is granted only to the users of the role senior analyst. Reports have to be reviewed and approved in order to obtain status released. Only released report templates can be used.	2/1/2	4

Requirement of data flow/step	Potential Failure Mode/	Potential Effect	Severity/ Probability/ Detectability	Overall Risk	Mitigating Action / Control	Severity/ Probability/ Detectability	Final Overall Risk
Reports must include sufficient metadata to support reconstruction of entire data history	There is no sufficient metadata	The reports are no attributable	3/2/3	18	The reports are configured in a way that all the necessary data about the result is displayed. It is included the name of the product and the standard, the number of the task, appropriate information about the instrument and the method, the name and the role of the user, the time of performing the task, and the electronic signatures.	2/1/3	6
Electronic reports must show electronic signatures	Electronic records do not show electronic signatures	Electronic records are not reliable	3/2/3	18	The reports are configured to show electronic signatures, which include the name of the user, the role, the time of review and approve and appropriate comment.	2/1/3	6
It must be possible to back up and restore all data from the system	No back up or restore possible	Data cannot be backup or restored	3/2/3	18	Backup and restore available for LabX	2/1/2	4
It must be possible to setup rules for automatic back up which run at specified intervals	Automatic back up cannot be set	The data cannot be backup at specific time	3/2/3	18	The backup and restore are setup according to defined procedure for back-up and restore	2/1/2	4

Configuration of the software

Restrict access

As highlighted in the GMP guidelines it is fundamental to restrict access to computerized system to authorized persons (EudraLex, 2011b; 21 CFR part 11). Since Labx can integrate with active directory, it means that a single sign-on is possible for the application. The system enforces that each individual user must have a unique user identity. Using active directory service, the user properties and password management are delegated from Windows to LabX environment. That means that the security settings are the same as the global security policy through the system.

User management

One of the initial steps of configuring the computerized system is defining the user management and assigning the rights to different user groups. Considering that LabX is used for routine analysis in QC laboratory, various users with different functions are involved in the acquisition and processing of electronic data. Therefore, a clear assignment of users, roles and privileges should be defined and documented and only registered and authorized users should have access to the system (Agit, 2018; WHO, 2021). Full use should be made of access controls to ensure that people have access only to functionality that is appropriate to their job role (MHRA, 2018).

LabX software enables adding, changing, deleting or temporarily disabling the users. Users are grouped in roles, and each role can be assigned with different rights and responsibilities. Each user can be assigned at least one role. The rights assigned to the roles can be subdivided by system and modules, like LabX balance. The first step of configuration of the user management is defining the roles that will be used in the system. The use of the system is principal consideration when creating the roles. Due to the fact that the system will be used for routine analysis, and the results will be used for release or stability testing, four groups of users which will be involved in the analysis are created. Access and privileges are in accordance with the role and responsibility of the individual with appropriate controls to ensure data integrity (WHO, 2021).

The software connects instruments which require managing of specific resources related to the instruments. For the analytical balances those resources are weights that are used for calibration and daily check of the balances. The role maintenance is created with main purpose of managing of those specific resources, because the users of that group are responsible for defined calibration of the weights. The rights that are assigned to the group maintenance are integral part of their job role.

System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) are not assigned to individuals with a direct interest in the data (data generation, data review or approval) (MHRA, 2018). The group IT support includes system administrators responsible for use registration and assigning defined access rights (Agit, 2018). Also, the group IT support has assigned rights for configuration of the system, editing security settings as well as adding instruments to the system. IT support supervises the back-up and restore of the system and handles the incidents related to the software (EudraLex, 2011a). The users in this group are not included in other groups in order to avoid conflict of interest (Agit, 2018; WHO, 2021). System administrator access is restricted to the minimum number of people possible (MHRA, 2018)

Data obtained in the software cannot be deleted, which means that neither of the role groups can have this possibility. Only the group IT support has assigned privilege of deleting methods and report templates, but only after previous review and approval of the responsible users. This is because certain privileges should not be assigned to administrators without justification, and such activities should only be done with authorization by another responsible person (WHO, 2021)

Signature policies

Signing procedures in the software can be defined for approval of versioned objects. The signing procedures are activated and objects cannot be released until all required signatures have been obtained. If objects are edited new versions are generated. Released versions however will remain the active versions. The option Auto release is activated and objects are released by the system as soon as all required signatures have been obtained. There are three options for signatures policies. The first is no signing procedure which means that the object will immediately change to approved. The second is requirement of one signature to fulfill the policies. And the third one is that two signatures are required to fulfill the policies. The approval state of and object will change to reviewed after the first signature and to approved after the second signature (LabX OI, 2019). In order to implement appropriate controls for electronic documents, the signing policies are configured with requirement of two signatures. The signing role for the first signature can be defined and in software configuration that role is reviewer, and for the second signature is approver. Only members of the selected roles are allowed to sign. The option for different user required is selected and that means that reviewer and approver must be different user, and the same user who signed the previous step cannot sign for this step. Laboratory records containing test results should be reviewed by a designated second person after a test has been concluded. There are also requirements for inspectors regarding the review of documents by a second person. They are supposed to verify whether this review has been carried out by a suitable and independent second person (Pommeranz, 2019)

There is an option for selecting whether comments are mandatory for signature step (LabX OI). Considering that guidelines outstand that for all changes a meaningful reason should be given and recorded in the audit trail, entering a comment is set up to be mandatory when signing (Agit, 2018). LabX has the possibility to revoke or remove an electronic signature of the result sets. This ability is only given to authorized individuals via the access control privileges. In rights and privileges roles reviewer and approver have authorization to revoke approval.

Audit Trail

Audit trail is one of the most important functionalities of the computerized system which is emphasized by all regulatory bodies is audit trail. An audit trail provides a secure recording of life cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. (WHO, 2021; 21 CFR part 11; OMCL, 2018a). The audit trail allows reconstruction of the course of events relating to the creation, modification or deletion of an electronic record (Agit, 2018). The audit trail should include the following parameters: details of the user that undertook the action; -what action occurred, was changed, incl. old and new values; -when the action was taken, incl. date and time; -why the action was taken (reason); and in the case of changes or modifications to data, the name of any person authorizing the change (PIC/S, 2021). The audit trail should be an additional unalterable electronic record. It should be linked to the electronic raw data in a logical or physical way. Regardless of the technical solution the audit trail should be inseparably linked to the corresponding electronic raw data and have the same retention requirements (Agit, 2018).

The function Audit Trail in LabX software records all important activities to provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. This function enables auditing of data access, deletions, changes and manipulations. Audit Trail entries include information such as user identifications, time stamps and workplaces (LabX OI, 2019). Since users must not be allowed to amend or switch off the audit trails or alternative means of providing traceability of user actions, actions triggered by the system are allocated to system users and not to known users managed in the user management (LabX OI, 2019; OMCL, 2018a). This means that Audit trail is unalterable by users using the application and access to modify the audit trail entries in the database via the operating system is not possible. According to that, there is no possibility to assign privileges to any group of users of modifying or deleting audit trail, so the software is initially designed to protect the audit trail from unauthorized modifications. The only privilege considering audit trail, that can be granted to the users, is 'view' audit trail, and the software is configured for all the users can access to the audit trail.

The system should be able to print and provide an electronic copy of the audit trail, and whether viewing in the system online or in a hardcopy, the audit trail should be available in a meaningful format. If possible, the audit trail should retain the dynamic functionalities found in the computerized system, like search functionality and ability to export data such as to a spreadsheet) (PIC/S, 2021)

The audit trail in LabX software is searchable. The user can define its own filters, which will then be displayed in addition to the series of predefined filters. Creating own search folders makes it is easier to gain an overview of large amounts of data. Multiple criteria can be added to one search folder, and combinations can be created to meet several criteria (LabX OI, 2019). Audit trails are available for review and copying by regulatory authority, because there is possibility of printing out the audit trail on a paper or a PDF file can be generated by an authorized user (21 CFR 11).

Specific parameters of the software

Tasks

Performing analysis in LabX software is enabled through so-called tasks. Each task has unique ID in the software and every time an analysis is started, new task is created. Tasks contain information about methods, samples and the used instrument. The list of tasks may be viewed both on the instrument and on the PC. The task unique ID is used as the main identification for the obtained results and searching the results in the software is performed with the task ID. The unique ID enables data integrity through the whole life cycle of the data. The results and the audit trail can be searched by the task number which facilitates the process of data management. Only the certain groups of users which are directly involved in performing analyses, have granted rights to activate tasks. By disabling other users to perform tasks, the system is protected from unauthorized use of users, who do not have job description or sufficient knowledge for using the instruments of the system.

Methods

The analysis using an instrument connected to LabX can be performed by using a method. Method represents the program for executing the analysis. It consists of a series of method functions that are processed in sequence by the instrument. A method function usually comprises several sub steps which consist of parameters with changeable values. This means that methods are configurable, and functions that constitute the method can be chosen according to end-user's needs.

Method function result allows entering a formula which does calculations. Calculations are performed by using the results from the measurements which enables incorporation of the calculation in the system and elimination of spreadsheets (McDowall, 2022a). Also,

there is an option for entering measuring unit of the result, as well as decimal places that results are displayed. The number of decimal units are the same as the limits and acceptability criteria in the specification of analytical procedure (ISO/IEC 17025:2017). The formula is entered in the method and the calculation is done by the system at the moment of performing the analysis. Since only approved methods can be used, it is not possible to change the formula without previous approval. That enables protection of the calculation.

Methods are so-called "versioned objects". A new version is created every time the object is saved, which assures traceability of the methods that are used through the life cycle of the system and of the data (LabX OI, 2019).

The system enables grouping method in different folders. For improved manageability, naming of the methods and the way they are grouped in the method folders is defined by naming convention.

Reporting of the results

Considering that the methods in LabX software are configured to perform calculations, final results are reported from the software which enables all activities from weighing to reporting of the results to be executed automatically. This prevents inappropriately designed data process for small instruments that generate critical data, which is compounded by manually entering the weight into a computerized system or a spreadsheet, resulting in transcription error and inaccurate results (McDowall, 2022a) *Automating processes that acquire, process, calculate and report the results, ensures that the report meets integrity, quality, speed and compliance criteria (*McDowall, 2022b). Consequently, defined processes of reporting of data should be established in order to ensure accuracy and integrity of the results that are reported (GAMP, 2017; ISO/IEC 17025:2017*).*

The results from LabX software are available in workspace data where a list view of the results, result sets and reports is displayed. This list view represents search folder where the data can be searched by different search criteria as task number, instrument number, method name etc. In the list view results an entry is displayed for each sample processed and in result sets the results are grouped by the number of the task. The parameters of the results displayed in the results and result sets are built-in in the software and cannot be configured. When opening a task in the result set information about the measured sample, time of measurement, who performed the analysis, the name of the reviewer and approver, appropriate time stamps as well as the raw data of every step of performing the method is included (21 CFR 11; EudraLex, 2021; ISO/IEC 17025:2017). Thus, the record of the task includes complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 11). This information combined with the audit trail, assures reconstruction of every action of generating the result. (ISO 17025:2017)

Results can be also displayed in reports. The report templates can be configured and different report template is created for every method in the system. The naming of the report templates is defined with naming convention with purpose to facilitate searching of the reports, so that data can be retrieved for audit or inspection easily (McDowall, 2022b).

The report is designed to display the main calculated results and results from the measurements that are included in the calculation of the main result. The results are displayed in the same decimal unit and same measurement unit as required in specification. (ISO/IEC 17025:2017). Furthermore, the report includes name of the material or product and where applicable dosage form (EudraLex, 2011a). Report contains the type and internal number of the balance used which is reference to the utilized equipment (EudraLex, 2011a). The number of the task is displayed in the report, which facilitates searching of the result in the software (ISO/IEC 17025:2017). Displaying the basic parameters of the method, as the method name and method ID, which are unique for each method, enables connection of the results with the used method and calculations (21 CFR part 211; EudraLex, 2011; ISO/IEC 17025:2017). Also, the report contains the date of analysis, user name of the person who performed the analysis and user name of the persons who verified the results with appropriate comment (21 CFR part 211, EudraLex, 2011, ISO/IEC 17025:2017). Report templates that are used for reporting of the results are reviewed and approved by reviewer and approver and have status released. Reports that have status proposed cannot be used for reporting of the results. Adequately designing the reports enables accurately, clearly and objectively displaying the results in the report, including all the information necessary for the interpretation of the result (ISO/IEC 17025:2017).

Validation of calculations

Considering that LabX allows configuration of customized methods and reports, key actions need to be incorporated into the methods and reports provided they are validated and locked to prevent changes. Automated reporting tools and reports may reduce the checks required to assure the integrity of the data (MHRA, 2018). This means that input to and output from the computer or related system of formulas or other records or data should be checked for accuracy, because it is not appropriate to assume that the built-in function for calculation work as intended (21 CFR Part, 211, Phan, 2003).

All calculations are verified with a system completely independent from the software. The principle of validation method is to compare the results obtained by the software with results obtained by commercial software like excel, using the same dataset as input and any calculations should be critically examined (EudraLex, 2011a, OMCL, 2018b).

The validation of the calculation is performed by activating a method which contains calculations and performing appropriate measurements. When the method

is finished, the measurements of the performed task from the result set are entered in an excel spreadsheet. Check of the correctness of the displayed measurements in the result set is performed during software validation and it is out of scope during validation of the calculations. The same formula used in the method is applied in the excel and the calculation is performed. The results obtained from the software and from the excel are compared. The acceptance criteria are set that there should be no difference between the results taking into consideration the rounding criteria. If there are differences between the results, the entered values are checked, the formula is checked and the rounding of the excel is checked. The data in excel are labeled in the same manner as in the software, which allows traceability between the two calculations. All the steps of the validation need to be documented. The validation is documented with print screens of the calculated values form the software and from the excel, print screen of the formula used and print screen of the result. A sufficient amount of data evidence must be collected to ensure that a third party-reviewer can derive the same conclusion as those who performed the actual validation (Phan, 2003).

The formula and the result are entered in an appropriate document which must be signed by the performer of the validation, and the responsible persons. After approval of the validation, the method is reviewed and approved and gains status released and can be used for routine work.

Conclusion

This paper explains the configuration of the computerized system utilized in the GMP environment. When configuring the system, the principal directions of the guidelines were followed in order to fulfill data integrity principles. All the critical points which can be potential risk for data integrity were evaluated. and appropriate mitigating action was implemented in the configuration of the software. The manner which computerized system is configured increases the security of the data and establishes controlled workflow. Creating methods which perform calculations reduces the time necessary for calculations, and their validation and verification for suitable use enables security and correctness of the obtained results. This makes the process of analysis more effective by reducing the possibility of human error and allowing for more detail via automation. At the end, adequate and carefully configured computerized system followed by proper validation, increases the data integrity, facilitates the analysis and reduces the time of review.

Acknowledgement

The author would like to thank Alkaloid AD-Skopje, Pharmaceutical, Chemical and Cosmetics Company for support, comments and suggestions made during the process of writing this paper.

References

21 Code of Federal Regulations (CFR) Chapter I, Subchapter C, Part 211. Current Good Manufacturing Practice for Finished Pharmaceuticals. Available at: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211 Assessed: 23.10.2022

21 Code of Federal Regulations (CFR) Chapter I, Subchapter A, Part 11. Electronic Records; Electronic signatures. Available at: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 Assessed: 15.10.2022

21 Code of Federal Regulations (CFR) Chapter I, Subchapter H, Part 820. Quality System Regulation. Available at: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-820 Assessed: 15.10.2022

Agit, 2018a. Guidelines for the Acquisition and Processing of Electronic Raw Data in a GLP Environment. Good Laboratory Practice. Swiss Working Group on Information Technology in a GLP Environment. Available at: https://www.anmeldestelle.admin.ch/chem/en/home/themen/gute-laborpraxis/agit.html Assessed: 15.10.2022

Agit, 2018b. Guidelines for the Development and Validation of Spreadsheets. Good Laboratory Practice. Swiss Working Group on Information Technology in a GLP Environment. Available at: https://www.anmeldestelle.admin.ch/chem/en/home/themen/gute-laborpraxis/agit.html Assessed 15.10.2022

Agit, 2018c. Guidelines for the Validation of Computerized systems. Good Laboratory Practice. Swiss Working Group on Information Technology in a GLP Environment. Available at: https://www.anmeldestelle.admin.ch/chem/en/home/themen/gute-laborpraxis/agit.html Assessed: 15.10.2022

Chandra, S.D., 2021. Overview of Regulations on GMP Computerized Systems. World. J. Pharm. Res. 8 (10), 618-629 Available at: https://doi.org/10.20959/wjpr201910-15718

Churchward, D., 2015. Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 1, MHRA Inspectorate Blog. Available at: https://mhrainspectorate.blog.gov.uk/2015/06/25/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-1/

EudraLex, 2011a. Chapter 4: Documentation. The Rules Governing Medicinal Products in the European Union, Volume 4. Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Available at: https://health.ec.europa.eu/system/files/2016-11/chapter4_01-2011_en_0.pdf

EudraLex, 2011b. Annex 11: Computerized Systems. The Rules Governing Medicinal Products in the European Union, Volume 4. Good Manufacturing Practice Medicinal Products for Human and Veterinary Use/ Available at https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf

EudraLex, 2015. Annex 15: Qualification and Validation. The Rules Governing Medicinal Products in the European Union, Volume 4. EU Guidelines for Good Manufacturing Practice Medicinal Products for Human and Veterinary Use. Available at: https://health.ec.europa.eu/system/files/2016-11/2015-10_annex15_0.pdf

FDA, 2018. Data Integrity and Compliance with Drug CGMP, Questions and Answers, Guidance for Industry. Available at: https://www.fda.gov/media/119267/download

GAMP, 2017. Records and Data Integrity Guide. ISPE/GAMP. Available at: https://ispe.org/publications/guidance-documents/gamp-records-pharmaceutical-data-integrity

GAMP, 2022. A Risk-Based Approach to compliant GxP Computerized systems. ISPE/GAMP, GAMP 5. Second Edition. Available at: https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition

ICH, 2000. Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients, Q7. ICH Harmonised Tripartite Guideline Available at: https://database.ich.org/sites/default/files/Q7%20Guideline.pdf

ICH 2005, Quality Risk Management, Q9. ICH Harmonised Tripartite Guideline. Available at: https://database.ich.org/sites/default/files/Q9%20Guideline.pdf

ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. Available at: ISO - ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories

Labx, 2019. Operating instructions.

McDowall, R., 2022a. Why digitalize your laboratory? LCGC. Available at: https://www.technologynetworks.com/tn/ebooks/why-digitalize-your-regulated-laboratory-367668

McDowall, R., 2022b. Data Reporting, Integrity and Compliance. Technology Networks. Available at: https://www.technologynetworks.com/informatics/articles/data-reporting-integrity-and-compliance-367511

MHRA, 2018. GXP Data Integrity Guidance and Definitions. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

OMCL, 2018a. Validation of Computerized Systems. PA/PH/OMCL (08) 69 R7. Available at: https://www.edqm.eu/en/quality-management-qm-documents

OMCL 2018b. Annex 1 – Validation of Excel Spreadsheet. PA/PH/OMCL (08) 87 R6. Validation of Computerized Systems. Available at: https://www.edqm.eu/en/quality-management-qm-documents

Phan, T.T., 2003. Technical Considerations for the Validation of Electronic Spreadsheets for Complying with 21 CFR Part 11. Pharm. Technol. 27(1), 50-62. Available at: https://alfresco-static-files.s3.amazonaws.com/alfresco_images/pharma/2014/08/22/7432aebb-9f08-40f2-aa06-039b05f0fd6a/article-42756.pdf.

PIC/S, 2021. Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments. PI 041-1. Pharmaceutical Inspection Convention Co-Operation Scheme. Available at: https://picscheme.org/docview/4234

PIC/S, 2022. Guide to Good Manufacturing Practice for Medicinal Products Part II. PE 009-16 (Part II). Pharmaceutical Inspection Convention Co-Operation Scheme. Available at: https://picscheme.org/docview/4589

Pommeranz, S., 2019. GMP Documentation. GMP Journal 24. Available at: https://www.gmp-journal.com/current-articles/details/gmp-documentation.html

WHO, 2021. Annex 4, Guideline on Data integrity. WHO Expert Committee on Specifications for Pharmaceutical Preparations: fifty-fifth report. World Health Organization, Available at: https://apps.who.int/iris/handle/10665/340323

Резиме

Пристап базиран на ризик за интегритет на податоци при имплементирање на компјутеризиран систем во услови на ДПП

Марина Манџуковска Мицевска[1*], Ѓорѓи Петрушевски[1], Руменка Петковска[2]

[1]Алкалоид АД Скопје, Бул. Александар Македонски 12, 1000 Скопје, Северна Македонија
[2]Фармацевтски факултет, Универзитет „Св. Кирил и Методиј“, Мајка Тереза 47, 1000 Скопје, Северна Македонија

Клучни зборови: компјутеризиран систем, интегритет на податоци, проценка на ризик

Имплементирањето на компјутеризиран систем во лабораторијата на Контрола на квалитет, бара детално планирање на конфигурирањето, земајќи во предвид дека интегритетот на податоците мора да се одржува преку целиот животен циклус на компјутеризираниот систем. Со идентификување на критичните проблеми во однос на интегритетот на податоците и проценувајќи го можниот ризик во текот на целиот процес се овозможува воспоставување на соодветни мерки за обезбедување на интегритетот на подароците. Овие мерки се имплементирани во конфигурацијата на системот коишто ја зголемуваат безбедноста на податоците и воспоставуваат контролиран тек на процесот. Со креирањето на методи кои што изведуваат калкулации, се намалува времето потребно за пресметки, и нивната валидација и верификација за соодветна употреба овозможува сигурност и точност на добиените резултати. Овој процес ја зголемува ефективноста на анализата, преку намалување на можноста за човечка грешка и овозможува повеќе детали преку автомизација. На крај, адекватен и внимателно конфигуриран компјутеризиран систем, проследен со соодветна валидација, го зголемува интегритетот на податоците, ја олеснува анализата и го намалува времето за преглед.