VALGENESIS®

WHITE PAPER

21 CFR PART 11 COMPLIANCE ASSESSMENT

Overview

Based on the increased use of computer systems in the pharmaceutical industry, the United States Food and Drug Administration (US FDA) issued the 21 CFR Part 11 regulations in March of 1997. This regulation provides the criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper.

The intent of the 21 CFR Part 11 rule is to define controls for computer systems and to encourage the greatest possible use of electronic technology while still allowing the FDA to follow its mandate to protect public health. This regulation outlines the controls necessary for those that choose to utilize electronic records and electronic signatures. It establishes criteria for the creation and management of electronic records and electronic signatures. This paper contains information about the FDA ruling as well as how ValGenesis VLMS (Validation Lifecycle Management Systems) meets 21 CFR Part 11 requirements.

TABLE OF CONTENTS

Complying with 21 CFR Part 11 Requirements

For FDA regulated companies that use electronic records and electronic signatures, as well as submit them to the FDA for purposes of seeking their approval of processes and products, are required to comply with 21 CFR Part 11.

Regulations are required to ensure the following:

1. *The authenticity, integrity, and confidentiality of electronic records are not compromised from the initial creation to the point of receipt by the FDA*
2. *The system generates accurate and complete copies of records that the FDA can inspect and review*
3. *Electronic records are secure and easily retrievable*
4. *Only authorized individual can access, modify and electronically sign the electronic records*
5. *A log of all changes made to the electronic records will be maintained throughout the lifecycle of the document*
6. *The business process is enforced in the desired sequence and each step of the process is performed in the proper sequence*
7. *Electronic Signatures with date and time stamps are recorded, stored, and attached to changes made*
8. *Persons developing, maintaining, and using the electronic records or the electronic signing system are properly trained*
9. *Persons using the system are accountable for any action conducted in the system under their electronic signatures*
10. *SOPs are established and maintained in regard to all of the above requirements*

Security Features of ValGenesis VLMS System

ValGenesis has been designed with the most advanced security features available on the market to date. Through its rich array of security features, ValGenesis VLMS system provides clients with the security features needed to operate in the highly regulated FDA space. Each of the security features is explained in greater detail below.

Username / Password Authentication

ValGenesis requires that each user log in to the application through a unique username and password combination. For added security, ValGenesis generates a unique identification number for each username registered in the system. Additionally, every password is encrypted to avoid identity theft.

ValGenesis provides the System Administrator with the flexibility to define a password policy with regards to password length, complexity level, expiration period, password expiration alert notification details, and the number of previously used passwords stored in the password history log. ValGenesis enforces password confidentiality by requiring the user to create a new password on first login. This password is encrypted and stored in the system, thereby providing additional password security.

Electronic Signatures

ValGenesis provides users with the ability to use electronic signatures. Electronic signatures increase the security of the application, as they can be used to manage a wide range of approval and change control processes in compliance with 21 CFR Part 11.

The electronic signature has additional features that further enhance security, such as the display of the current user logged in to the application, the specific activity that the user is electronically signing, or approving a document, and the encrypted username and passwords.

The system also features signature manifestation, where the signer has the ability to provide an explanation for the meaning of the signature.

Security Profile Settings

From the Security Profile, the security options of ValGenesis VLMS can be configured to meet corporate policies and procedures. As noted previously, the login password security settings can be set from this profile.

ValGenesis System Administrator can configure the system to lock out users after a specified number of consecutive invalid login attempts. This feature minimizes the possibility of successful brute force attacks. Once an account has been locked out, the lockout information is recorded in an audit trail. The owner of the account that has been locked out must contact the System Administrator to reset the password. Upon logging in for the first time after the password has been reset, ValGenesis VLMS will force the user to create a new secure password.

ValGenesis can also be configured to log out users and terminate sessions based upon a specified period of inactivity. The purpose of this feature is to prevent unauthorized use of the application when the account owner has left the workstation without logging out.

Access Control and Role Based Security

ValGenesis restricts access to menus and functions to specific users based on their role. This is configured in the User Profile settings. ValGenesis does not restrict users to configuring the system to a specific set of parameters. Instead, users can configure ValGenesis to meet their application needs. It does not impose maximum size limitations on the number of user roles and groups.

Controlled Workflow

ValGenesis has been designed to enforce process sequences, such as the business process flow of validation. It provides the interlocks necessary to ensure that validation activities are performed in the required sequence, such as approval of step 1 is a prerequisite for the approval of step 2. Or that step 1 and step 2 can proceed in parallel but would need to be completed before step 3 can start.

The design of ValGenesis is such that on completion of prerequisite tasks, the person assigned for the subsequent task may be notified via email so as to ensure alerts have been fulfilled, the assigned user of the next task will be alerted through the ValGenesis message alert feature.

Audit Trails

ValGenesis audit trails are designed to track activities such as user login and logoff, password changes, changes to security, user and global profile settings, failed login attempts, etc. These audit trails contemporaneously capture the username associated with the activity along with the system generated date and time. The user cannot turn off the audit trail while ValGenesis is in operation.

ValGenesis VLMS and 21 CFR Part 11

In the Life Sciences industry, compliance with 21 CFR Part 11 regulation is mandatory. ValGenesis was designed and developed to comply with this regulation. This section enumerates how ValGenesis meets the requirements of 21 CFR Part 11 requirements.

Requirement 11.10 (a)

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

ValGenesis has been designed and developed using SDLC (Software/System Design Lifecycle) methodology. Its development conforms to the process described in US FDA's document titled General Principles of Software Validation: Final Guidance for Industry and FDA Staff, dated January 11, 2002.

ValGenesis serves as a document repository to provide the necessary documented evidence that systems and process have been validated. Inherent in ValGenesis's design is the enforcement of sequencing validation activities to include review and approval of documents for the design, development, test, and deployment of systems complete with documented results of Risk Assessment and Requirements to Test Traceability Matrix (RTTM).

Requirvement 11.10 (b)

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

ValGenesis records are electronic and are stored in a native format. ValGenesis presents these records in a Human Readable Format (HRF). These HRF records may be printed and/or copied to different types of portable media on demand.

Original records, which are stored as binary objects along with their metadata, are also copiable.

Requirement 11.10 (c)

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

ValGenesis encrypts and stores all data, including metadata and audit trails, in its database. These records may be retrieved accurately during the company's records retention period.

Requirement 11.10 (d)

Limiting system access to authorized individuals.

ValGenesis users obtain system access using a unique User ID and password combination. It also provides users the flexibility to implement a password policy to suit their business process needs. These include features such as minimum and maximum password length, password aging interval, reuse of passwords on password expiration, etc.

ValGenesis provides an Active Directory interface for user authentication. ValGenesis SaaS also provides Active Directory Federated Service (ADFS) and Single Sign On (SSO). User authorization is implemented through ValGenesis's configuration utility, where users may be assigned to groups. These groups have permissions to access certain functions only.

Requirement 11.10 (e)

Use of secure, computer-generated time-stamped audit-trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

ValGenesis tracks the creation, development, execution, modification and approval of all validation documents. These activities are audit trailed. All audit trail entries are linked to their parent record and can be retrieved and reviewed. Each audit trail entry includes the system generated date and time stamp of the occurrence of event, the type of action taken (addition, modification, deletion, approval, non-approval and user identities of the actions).

Requirement 11.10 (f)

Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.

By design, ValGenesis enforces the Validation life cycle activities. It also provides the ability to create workflows that automate business processes, such as document review and approval processes. The workflows can be used to ensure that the sequence of events prescribed in the organizational policies and procedures for a given process is strictly observed. Each step in a workflow only becomes available after all prerequisite steps are completed. When a workflow task is ready to be performed by a user, the task appears in the user's Message Alert Task List Window. Once completed, the next task in the workflow can be assigned to the applicable user.

Requirement 11.10 (g)

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

ValGenesis has a two-tiered security system, requiring the user to enter a valid User ID and password in order to gain access to the system. It is also equipped with role-based security that ensures only authorized users belonging to a specific role are capable of accessing specific functions.

Requirement 11.50 (a)

Signed electronic records shall contain information associated with the signing that indicates the printed name of the signer, the date and time of the signing, and the meaning associated with the signature (such as review, approval, responsibility or authorship).

ValGenesis prohibits user approval of a document without opening and reviewing the content. The "Approval" steps in a workflow indicate the meaning of the signature and the approver is required to either "approve and sign" or "reject" the document. It also requires the entry of the reason for rejection. A document cannot be rejected without a reason being attached for the rejection. When the document attached to the workflow is signed, the signing event is recorded in the audit trail logs. This signature audit trail contains the user's name, the date and time stamps of the signing, as well as the meaning of the signing, and a link to the signing workflow.

Requirement 11.50 (b)

The items identified in requirement 11.50(a) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of electronic record (such as electronic display or printout).

The signature information is linked to the document as metadata. When a user approves the document, the user's name, title, date and time, and meaning of the signature are "stamped" onto the signed document. The electronic signature information can be viewed through reports

Requirements 11.70

Electronic signatures and handwritten signatures applied to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be removed, copied, or transferred to falsify an electronic record.

ValGenesis provides comprehensive audit trails of user activities and links the electronic signature to the respective record. This electronic signature metadata associated with the document cannot be removed or overwritten.

Requirement 11.100 (a)

Each electronic signature will be unique to an individual and shall not be reused by or assigned to another individual.

The ValGenesis security system ensures that authorized users have a unique username and password combination. To enhance security, ValGenesis attaches a unique User ID number to the username and stores this information in the database. Usernames can never be reused even if they are deactivated.

Requirement 11.200 (a) (i)

Electronic signatures not based upon biometrics shall employ two distinct identification components such as an identification code and password.

ValGenesis utilizes a unique combination of username and password as the two components of the electronic signature.

Requirement 11.200 (a) (1) (i)

When executing a series of signings during a continuous period, the first signing shall be executed using all signature components and subsequent signings at least one signature component.

ValGenesis users are required to login to the system using the two-component login consisting of the User ID and password. Once logged in to the system, all subsequent activities such as document approval/ rejection is realized via an electronic signature window that appears on the screen. The User ID is prepopulated in this window and the user is expected to enter the appropriate password.

Requirement 11.200 (a) (1) (ii)

When an individual executes one or more signings not performed during a continuous period, each signing shall be executed using all of the electronic signature components.

A user performing one or more signings in a non-continuous manner, ValGenesis requires reauthentication using both User ID and password.

Requirement 11.200 (a) (2) (3)

Electronic signatures shall be used by their genuine owners and be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

User login is required for a password change. On account lockout resulting from consecutive login failures, the System Administrator is required to unlock the account to reactivate it. On reactivation, the user will be required to create a new password.

Requirement Section 11.300 (a)

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

ValGenesis ensures that all usernames assigned to users are unique. If a username is deactivated, ValGenesis VLMS will not allow the username to be reissued to another user.

Requirement Section 11.300 (b)

Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging).

The ValGenesis System Administrator is capable of configuring the 'password expiration' period in accordance to the organization's policies and procedures. When the period of password validity is near expiration or expired, the user will be prompted to create a new password in accordance with the password complexity configuration for the system. When a user that has electronically signed a record is deauthorized from electronic signature, his/her electronic signature records will remain attached to the associated records for as long as the record exists in the system.

Requirement Section 11.300 (c)

Following loss management procedures to electronically deauthorize lost, stolen, or compromised tokens, cards, and other devices that bear or generate identification code and password information and provide for the issuance of temporary or permanent replacements using suitable, rigorous controls.

ValGenesis is equipped with the capability to deactivate users by the System Administrator.

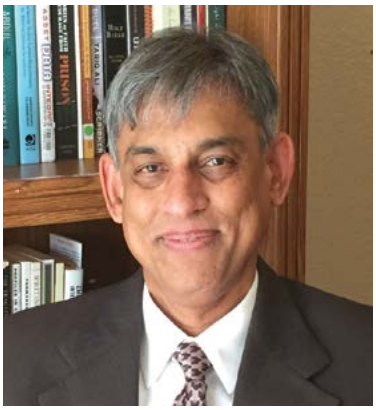
Requirement Section 11.300 (d)

Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

ValGenesis login requires a valid username/password combination. After consecutive failed login attempts (configurable by the System Administrator), the account will be locked. Locked accounts require the user to seek the assistance of System Administrator to unlock the account. To log in to the unlocked account, the user can log in to the system with the assigned temporary password and will be required to create a new password on first login. This new password will be required to adhere to the password policy configured for the system.

In Conclusion

ValGenesis is designed to comply with 21 CFR Part 11. With advanced security features, it improves the efficiency of the validation effort and provides users significant savings in validation time. It removes the human factor from validation to a significant degree, thereby boosting data integrity. Its features satisfy data integrity attributes such as attributability, legibility, contemporaneous recording of activities, consistency of validation procedures, and originality by storing both raw data and metadata automatically onto enduring media. Its data is available on demand by those who need it (and when they need it) since the data is copiable onto portable media and also available in the Cloud.



Chinmoy Roy is a biopharmaceutical consultant with over 38 years of experience in CSV, Data Integrity, 21 CFR Part 11, Annex 11 and manufacturing process automation. He is a member of ISPE's Data Integrity Special Interest Group (S.I.G). He travels the world to train industry personnel in the areas of his subject matter expertise as well as to conduct data integrity audits. His presentations blend his field experience to highlight the intricacies of implementing regulations. Chinmoy has a bachelor's degree in Electrical Engineering and a Master's degree in Computer Science. He lives in the San Francisco bay area.

ValGenesis, Inc. is the creator of an innovative software platform that serves as a foundation for managing compliance-based validation activities in life science companies. ValGenesis, Inc. is the provider of the first enterprise application that manages the corporate validation lifecycle process. This solution is fully compliant with U.S. FDA 21 CFR Part 11 and Annex 11 requirements. As the first fully paperless solution for electronic management of validation execution and approval, ValGenesis was selected by an industry peer review committee to receive the Parenteral Drug Association (PDA) New Innovative Technology Award in 2005.

VALGENESIS®

www.valgenesis.com