VALIDATOR

COMPLIANCE associates

VALIDATOR WHITE PAPER

Addressing 21 CFR Part 11

1 INTRODUCTION

21 CFR Part 11 has been become a very large concern in the pharmaceutical industry as of late due to pressure from regulatory bodies enforcing compliance for GxP systems. Due to this, more and more organizations are realizing the criticality of employing or ramping up existing system to meet these requirements.

This document's intent is to clearly define how the Validator system developed by Compliance Associates demonstrates full compliance with 21 CFR Part 11 requirements.

2 SCOPE

Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act), even if such records are not specifically identified in Agency regulations (§ 11.1).

3 ELECTRONIC RECORDS

Validator is a true content management system that allows documents, templates, sections, and other data to be created, manipulated and repurposed within the system with ease to quickly produce deliverables. Any deliverable produced by the system can in turn be generated as a report as well. These deliverables can be viewed in screen within data components, generated and saved as PDF copies, and printed from the PDF copies as well.

4 AUTHORIZATION, ACCESS AND ENCRYPTION

Validator employs three forms of identification that are required in order for users to login and access projects; User ID, Password, and Certification ID. Certification ID's are generated as a result of reading through training material content pertaining to validation, and taking an online test available through the system. A passing grade will generate the certificate ID which can then be used to login.

User passwords are encrypted in the database using irreversible hash encryption algorithms, which ensures that passwords can never be discovered when created, even on the back end.

The web.config file that holds configuration settings for the application also have all key database connection strings and security parameter encrypted for security

The scope of Validator implementation currently is local installation at a client facility and thus is considered a closed system. As a result of this, responsibility for the network security and external access through VPN for secure connection falls to the client.

Compliance Associates does not currently provide a hosted solution for Validator and thus the requirements pertaining to security of Validator as an open system will not be covered in this document.

5 ELECTRONIC SIGNATURES

Validator employs e-signatures at several key locations in the system and most importantly during the review and approval of deliverables in the workflow module.

E-signatures in Validator use a combination of User ID and password, both of which are required upon each signature regardless of continuous or separate signing sessions.

Once a user signs electronically, a record is created in the database along with the User ID, time and date of signature and meaning of signature. When signing as approval for documents, the record information is also embedded within the PDF, and the database record will also contain information about the report being approved, the version etc. This report signature record is then encrypted within the database to secure the link between the record and the PDF, and prevent any tampering even on the back end by administrators.

Furthermore, PDF's generated in Validator are stored in binary format and cannot be edited from within the database. PDF's stored in the system repository can be viewed by users and administrators, but any modifications made to the PDF are not able to be saved back to the database. This prevents unauthorized modification of PDF documents by system users and administrators.

The combination of locked down PDF and encrypted records from signatures preserves the two core components of the e-signature in Validator producing secure and compliant methodology of signing documents.

6 SSL ENCRYPTION

Validator employs SSL encryption to ensure that any page that allows login or signature within the system has been securely encrypted to use the "https" protocol on URL's to disallow any tampering, hacking or hi-jacking of data over networks or opens systems.

7 SPECIFIC INERPRETATION TO RULING

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
		Controls for Closed Systems	
.10	Controls for Closed Systems	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Validator allows application administrators to define roles/ permissions for each view within the system. Authenticity, integrity and confidentiality of electronic records within CA Validator are maintained through permission levels that restrict access where applicable. Documents are controlled and recorded in a secure audit trail. Authentication involves userid, password and certification id.
.10(a)	Validation	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Compliance Associates currently does not offer the Validator system as a hosted solution. Installations are done at client sites, thus the responsibility of validating the system lies with the client. However Compliance Associates has a complete validation package that is made available to clients upon installation such that this compliance requirement can be met fully.
.10(b)	Readability	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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Validator allows the viewing, generating and printing of reports for any deliverable produced by the system. Please refer to Section 3 of this document.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
.10(c)	Archival Record Protection	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Validator includes comprehensive security measures to protect all electronic records within the system. All reports generated, even for closed projects is secured, organized and readily available from the Validator repository when needed. Validator also has an archiving feature to relocate and store legacy reports/ projects to a shared drive location.
.10(d)	System Security	Limiting system access to authorized individuals.	Validator provides multiple levels of security, restriction of access to projects, administrative functions, and every individual page in the system by role. Refer to Section 4 of this document for more details.
.10(e)	Audit Trails / Document Retention	Use of secure, computer-generated timestamped 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 shall be available for agency review and copying.	Validator contains two levels of audit trail, one for the application and one for report approval. Both audit trails capture user performing the action, and date and time of the action. The application audit trail preserves prior entries and report audit trials capture meaning of signature. Audit trails within Validator are secure and are not alterable by users or administrators. Administrator module actions are also captured within a separate audit trail.
.10(f)	Sequencing	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Validator allows multiple points at which dependencies can be set. Foremost document sequence can be pre-set to force sequencing of events and deliverable creation based on the organization's needs. Test procedure dependencies are also possible.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
.10(g)	Authority Checks	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.	Please refer to Sections 3, 4 and 5 of this document.
.10(h)	Location Checks	Use of device (e.g. terminal checks) to determine, as appropriate, the validity of the source of data input or operational instruction.	Validator currently has no external systems or interfaces that data flows in from or out to.
.10(i)	Education/ Training	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Validator provides a computer based training module. Upon completion of computer-based training, the user can choose to take a test. If the score is a passing grade then the user is provided with a unique certificate id. This unique certificate id grants the user access to the system. This method of restrict access to trained individuals ensures that the regulations that dictate the delivery and management of training is adhered to.
.10(j)	Written Policies	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The compliance responsibility of this requirement lies with the client implementing the Validator system.
.10(k1)	Document Controls/ Audit Trials	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	The compliance responsibility of this requirement lies with the client implementing the Validator system.
.10(k2)	Document Controls/ Audit Trials	Revision and change control procedures to maintain an audit trail that documents timesequenced development and modification of systems documentation.	Compliance Associates provides detailed release notes documentation on major and minor product releases. Compliance Associates also employs a robust change control procedure internally that links to support calls made that allows clients to understand the impact of change requests and future releases.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
		Controls for Open Systems	
	Open System Controls	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and when appropriate, the confidentiality of electronic records from the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	Validator provides encryption for userid / password combinations and the use of electronic signatures. Please refer to Section 5 of this document for more details.
		Signature Manifestations	
.50(a)	Name Display/ Purpose	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: The printed name of the signer; The date and time when the signature was executed; and The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Electronic singatures in Validator include name, date/time of signing and meaning of signature within the electronic record generated upon signing, and also on the PDF generated.
.50(b)	Name Display	The items identified in paragraphs (a) (1), (a) (2), and (a) (3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic records (such as electronic display or printout).	Each electronic record is stamped with name, time and date stamp.
		Signature/Record Linking	
.70	Signature Binding	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Electronic signatures in Validator generate records in the database that are encrypted and create PDFs with the embedded data that are stored in binary within the repository. Please refer to Section 5 of this document for more details.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
General Requirements for Electronic Signatures			
.100(a)	Electronic Signature Assignment	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Electronic signatures in Validator are done using User ID and password combinations used to login to the system which are unique, secure and encrypted.
.100(b)	Electronic Signature Assignment	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The compliance responsibility of this requirement lies with the client implementing the Validator system.
.100(c)	Certification to FDA Office of Regional Operations	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	The compliance responsibility of this requirement lies with the client implementing the Validator system.
Signature Manifestations			
.200(a1)	Bilateral Signature Security	Electronic signatures that are not based upon biometrics shall: Employ at least two distinct identification components such as an identification code and password.	Validator employs three components to sign electronically (user id, password, and certificate id). Please refer to Section 3 of this document for more details.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
.200(a1i)	Bilateral Signature Security	When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	All electronic signing performed within Validator requires at minimum, a User ID and password combination regardless of whether the session is continuous or not.
.200(a1ii)	Bilateral Signature Security	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all the electronic signature components.	All electronic signing performed within Validator requires at, minimum a User ID and password combination regardless of whether the session is continuous or not.
.200(a2)	Bilateral Signature Security	Be used only by their genuine owners; and	The compliance responsibility of this requirement lies with the client implementing the Validator system.
.200(a3)	Bilateral Signature	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.	Validator does not support the use of delegate signatures or deputization. Each user must sign for and approve only items they are responsible for and must use their own credentials to do so.
Controls for Biometric Signatures			
.200(b)	Biometric and /or behavioral-based signatures	Electronic signatures based upon biometrics shall be signed to ensure that they cannot be used by anyone other than their genuine owners.	Validator does not support biometric signatures.

7 SPECIFIC INERPRETATION TO RULING *(continued)*

PART §11.*	REQUIREMENT	TEXT OF 21 CFR PART 11	INTERPRETATION
		Controls for Identification codes/passwords	
.300(a)	Identification/ Password	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 should 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.	Electronic signatures in Validator are done using User ID and password combinations used to login to the system which are unique, secure and encrypted.
.300(b)	Identification Maintenance	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Validator has a configurable password aging feature built in and also contains password history control.
.300(c)	Identification Maintenance	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised token, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	The compliance responsibility of this requirement lies with the client implementing the Validator system.
.300(d)	Signature Security	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.	Validator locks out users after a set amount of failed login attempts and sends email notification to all users defined as administrators informing them of the unauthorized access attempts.
.300(e)	Identification Maintenance	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Validator does not support the use of tokens or ID cards as a means of authentication or any other function within the system.