Sievers* Soleil Rapid Bioburden Analyzer Software 21 CFR Part 11 Compliance

Application Note

Introduction

Part 11 of Title 21 of the Code of Federal Regulations applies to electronic records and signatures.[1] This application note is a section-by-section analysis of the 21 CFR Part 11 final rule and how the Sievers Soleil Rapid Bioburden Analyzer software complies with requirements for electronic records. For additional questions about these sections or concerns about Data Integrity, please contact your local Sievers representative or our technical support team at www.sieversinstruments.com.

Compliance with 21 CFR Part 11

21 CFR Part 11 Reference[1]	Question/Statement	Answer
Subpart B – Electronic Records §11.10 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:		
§11.10.a	Is validation of systems to ensure accuracy, reliability, consistent intended performance possible? Is there the ability to discern invalid or altered records?	*Yes, each assay generates a discrete electronic record in the form of an Assay Detail Report. The user can validate that each report is an accurate and consistent representation of the summary appearing on the software screen at the completion of the assay.* *Yes, the user can select a locked PDF option for assay detail reports to prevent alteration after generation. The locked PDF has limited permissions and the only permission allowed is to view and/or print the file.*
§11.10.b	Is the system able to produce complete and accurate copies of required electronic records in human readable form on paper for inspection, review, and copying by the agency?	*Yes, assay detail reports are available in a secure portable document format to allow printing via any networked or local printer.*

[1] CFR - Code of Federal Regulations Title 21. Retrieved March 20, 2024, from https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11?toc=1

21 CFR Part 11 Reference[1]	Question/Statement	Answer
§11.10.c	Are records protected to enable their accurate and ready retrieval throughout the records retention period?	*Yes, standard Windows security configurations can be used to prevent file deletion by users responsible for operation of the analyzer. The same configurations can also be used to establish a system administrator role that can move files for archival per the company's data retention policies. System administrator roles should be assigned to personnel independent from those responsible for the record content.* *Combined with the ability to create locked PDF records, these security features ensure accurate and ready retrieval of the primary records.*
§11.10.d	Is system access limited to authorized individuals?	*Yes, access to the system is limited to user IDs that are established and maintained within the software. User IDs require password authentication for access and controls are implemented to ensure that each user can securely define their unique credentials. Password rules can be configured within the software.*
§11.10.e	For each type of record in the system, is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify or delete electronic records?	*Yes, an independent audit trail captures all actions executed within the software and includes details on the event date and time, the user ID executing the action, details on the action, and when applicable a record of the original and new values resulting from an action.*
	Are controls in place to ensure that record changes do not obscure previously recorded information?	*Yes, the audit trail is generated in an encrypted format to prevent alteration, thus ensuring a continuous record without obscuring prior entries.*
	Is audit trail documentation able to be retained for a period at least as long as that required for the subject electronic records?	*Yes, like assay detail reports, standard Windows security configurations can be used to prevent audit trail deletion and ensure the audit trails are available for at least as long as what is required for the electronic records.*
	Is the audit trail available for agency review and copying?	*Yes, the audit trail can be exported as a locked PDF for review and copying.*

21 CFR Part 11 Reference[1]	Question/Statement	Answer
§11.10.f	Does the system use operational system checks to enforce permitted sequencing of steps and events, as appropriate?	*Yes, most applicably, the Daily Procedures and Run Assay functions employ a sequence of steps that must be acknowledged by the user and logged in the audit trail to guide through testing steps.*
§11.10.g	Does the system use authority checks to ensure that only authorized individuals can use the system? Does the system use authority checks to ensure that only authorized individuals can electronically sign a record? Does the system use authority checks to ensure that only authorized individuals can access the operation or computer system input or output device or perform the operation at hand? Does the system use authority checks to ensure that only authorized individuals can alter a record?	*Yes, a combination of user ID and password is used to restrict access to authorized individuals. Three access levels are available for analysts, administrators, and service personnel with each catered to specific functions and aligned uniquely with each User ID.* *N/A – Electronic signatures are not currently supported other than providing record of user actions in the audit trail and ensuring that electronic records are attributable to the personnel generating the data.* *Yes, the user IDs assigned to one of the three distinct access levels ensures that only authorized individuals can execute specific operations relative to system inputs and outputs.* *Yes, while primary assay detail reports can be exported as locked PDFs to prevent alteration and encrypted audit trails cannot be altered, the system does restrict alteration of system parameters to authorized individuals with traceability in the audit trail.*
§11.10.h	Does the system use device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction?	*Yes, the software connection to the Soleil Bioburden analyzer is provided via USB and the software will perform system checks to ensure validity of the connection.*
§11.10.i	Is there a determination that <service> persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	*Yes, as it pertains to Sievers service personnel who access the analyzer to generate electronic records, certification programs provide evidence that the personnel are qualified to perform their assigned tasks. Certification documentation is available via audit.*
§11.10.j	Is there establishment of, and adherence to, written policies that hold <service> individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification?	*Yes, Sievers personnel execute cGMP training to emphasize the importance of data integrity and the use of instrumentation to support operations.*

21 CFR Part 11 Reference[1]	Question/Statement	Answer
§11.10.k	(1) Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	*N/A – Control and distribution of documentation provided by Sievers to support operation and maintenance of the Soleil Rapid Bioburden Analyzer are the responsibility of the company using the analyzer.*
	(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	*Yes, Sievers maintains revision control of documentation via a defined change control process with time-sequenced traceability to modifications after applicable approvals.*
§11.50 Signature manifestations		
§11.50.a	Do signed electronic records contain information associated with the signing that clearly indicates all of the following:	
	(1) The printed name of the signer?	*Yes, the User ID is displayed on the Assay Detail Report as well as the audit trail.*
	(2) The date and time when the signature was executed?	*Yes, entries on the data records such as assay start time, assay end time, and actions logged in the audit trail include the date and time linked to the operation the identified user executed.*
	(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	*Yes, relative to audit trail entries, the action executed by the identified user ID is detailed.*
§11.50.b	Are the items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	*Yes, the printouts of the Assay Detail Reports and the Audit Trails contain the same information relative to the User ID of the user, the date/time of execution, and the meaning of the action attributed to that user.*
§11.70 Signature/record linking		
§11.70	Are electronic signatures and handwritten signatures executed to electronic records 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?	*Yes, the User ID is linked to the Assay Detail Report. By exporting as a locked PDF, this ensures that the User ID information cannot be excised, transferred, or overwritten to falsify an electronic record and lose the attributable linkage to the person executing the testing.*

21 CFR Part 11 Reference[1]	Question/Statement	Answer
Subpart C – Electronic Signatures *§11.100 General Requirements*		
§11.100.a	Is each electronic signature unique to one individual and shall not be reused by, or reassigned to, anyone else?	*Yes, each User ID attributed to a full user name is unique and cannot be reused or reassigned, even if that User ID has been disabled or retired.*
§11.100.b	Does the system allow the <service> organization to verify the identity of the individual before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	*Yes, as it pertains to the establishment of Service level users who access the software, the system is designed to require a registration number and license key to create the User ID. The combination of registration number and license key is only issued to qualified service representatives as part of a certification program verifying the person's identity and capability to perform testing on the platform.*
§11.100.c	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.	*N/A – The Soleil Rapid Bioburden Analyzer software platform is not designed to utilize electronic signatures as a legally binding equivalent of traditional handwritten signatures. Rather, the critical attributes of Subpart C were embedded in the logic for user management as they pertain to system access and electronic record generation and maintenance.*
§11.200 Electronic signature components and controls		
§11.200.a	Do electronic signatures that are not based upon biometrics: (1) Employ at least two distinct identification components such as an identification code and password? i. 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.	*Yes, the combination of User ID and unique password documents all actions executed by the particular user when logged into the system.* *Yes, initial login to the system requires the use of the User ID and unique password to access the functions that are available for the particular user role. The user credentials are attributed to all actions executed in a continuous period of controlled system access until the point the user logs out or the system auto logs out at a time that can be established per company requirements.*

21 CFR Part 11 Reference[1]	Question/Statement	Answer
	ii. 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 of the electronic signature components.	*Yes, when the user logs out or the system auto logs out, it is required to log in with a User ID and unique password to comply with the requirements to use two distinct identification components when executing actions not performed during a single, continuous period of controlled system access.*
	(2) Ensure use only by their genuine owners?	*Yes, upon creation of a new user, the system mandates that the user reset their password upon first login. This ensures that only the particular user has access to their credentials. The same logic of requiring password change upon first login attempt applies if a user is deactivated and reactivated by an administrator.*
	(3) Ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals?	*N/A – There are no mechanisms by which the user other than the one associated with the User ID and unique password can execute actions on behalf of the genuine owner.*
§11.200.b	Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	*N/A – The Soleil Rapid Bioburden Analyzer software does not support biometrics for user access, control, and management.*
§11.300 Controls for identification codes/passwords *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:*		
§11.300.a	Does the system maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	*Yes, each User ID attributed to a full user name is unique and cannot be reused or reassigned, even if that User ID has been disabled or retired.*
§11.300.b	Does the system ensure that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	*Yes, an administrator level user can configure password rules, including expiration after a defined number of days; lockout after a certain number of incorrect attempts; and prevention of using a specific number of past passwords.*

21 CFR Part 11 Reference[1]	Question/Statement	Answer
§11.300.c	Does the system electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	*N/A – The Soleil Rapid Bioburden Analyzer software does not utilize tokens, cards, or other devices that generate identification code or password information.*
§11.300.d	Does the system use 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?	*Yes, the software provides lockout controls if an unauthorized user attempts to access the system without the proper credentials. Only an administrator can reactivate an account and reactivation mandates that the user reset their own password prior to gaining entry at the next login attempt.*
§11.300.e	Does the system support 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?	*N/A – The Soleil Rapid Bioburden Analyzer software does not utilize tokens, cards, or other devices that generate identification code or password information.*

The principles of 21 CFR Part 11 and Data Integrity are closely related, if not entirely complementary, to one another. The above demonstrates compliance of the Soleil Rapid Bioburden Analyzer software as it relates to access control and management of electronic records. Additional concepts of Data Integrity extend much further and are discussed elsewhere. The concepts of Data Integrity continue to evolve and it is an exciting debate of ideas and concepts. The Sievers team encourages everyone to be engaged in the conversation and ongoing interpretation. For more information about how Sievers software can help you comply with new Data Integrity guidelines, please reach out to your local Sievers representative or visit our website, www.sieversinstruments.com.