Water Technologies & Solutions
fact sheet

21 CFR Part 11

Electronic Records and Signatures with the Sievers M9 TOC Analyzer and DataPro2 Software

introduction

Part 11 of Title 21 of the Code of Federal Regulations applies to electronic records and signatures[1]. This fact sheet is a section-by-section analysis of the 21 CFR Part 11 final rule and how the Sievers* M9 with DataPro2 software system complies. 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***
§11.10.a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. *DataPro2 can be validated and the data can be compared across the platform. Records cannot be altered. If the database is hacked, a series of checksums is used to detect invalid or altered files.*
§11.10.b	Is the system able to produce complete and accurate copies of required electronic records in human readable form on paper? *Yes via any networked or local printer* - Can a copy of a single record (in paper format) be supplied? *Yes* - Can a copy of the entire database (in paper format) be supplied? *Yes* - Are all parameters, such as status codes translated into human readable form? *Yes* - This includes audit trails and system documentation. *Yes*
§11.10.b	Is the system able to produce complete and accurate copies of records in electronic form for inspection, review and copying? *Yes, via proprietary or CSV format file* - Can a copy of a single record (in electronic format) be supplied? *Yes* - Can a copy of the entire database (in electronic format) be supplied? *Yes* - This includes audit trails and system documentation. *Yes*
§11.10.c	Are the records readily retrievable throughout their retention period –whilst valid and prior to archiving? *Yes* - Is there a back-up & restore process? *The system generates Database based files/data that may be backed-up by end users existing systems.* - Are records protected to prevent unauthorized modification or deletion? *Yes, via Database integrity check* - Is metadata also stored? *Metadata are data about data. The term refers to data used to aid the identification, description and location of networked electronic resources. Yes* - Can virus software installed and regularly updated to prevent data corruption? *Yes (user supplied)*

*Trademark of SUEZ, may be registered in one or more countries.

21 CFR Part 11 Reference[1]	***Question***
§11.10.c	Are the records readily retrievable throughout their retention period –once archived? *Mechanism/system dependent – long term archiving of application database data/files is by end user/IT department.* - Describe the data-archiving process? *See above.* - Do system users have access to archived data*? See above.* - Is metadata also stored? *See above.*
§11.10.d	Is system access limited by the system to authorized individuals? *Yes* - Is both a username/password required to access the system? *Yes* - What are the levels of access provided by the system? *Multiple authorization levels configurable by admin user*
§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* - Are audit trails created at the time of the transaction? *Yes* - How are time & date stamps established (including formats). *Computer time/date is used.* - Are all actions recorded – including system administrator activity? *Yes, audit trails exist and accessible with appropriate authorization level*
§11.10.e	Can the audit trail be modified? *No* - Is the audit trail outside of user access and control? *Yes* - Can it be switched off? If so how and is this recorded? *No* - Is audit trail integrity ever checked? *Yes, via database integrity check*
§11.10.e	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)? *Yes. Most electronic records cannot be changed. Previous values are recorded in audit trail for changeable fields.* - Can altered records be detected? *Yes, via database integrity check* - Is the original still visible? *Yes, via the audit trail* - Does the audit trail have a time & date stamp? *Yes* - Does the audit trail contain the reason for record modification? *Data records cannot be modified. Other data may be augmented with a comment.*
§11.10.e	Is an electronic record's audit trail retrievable throughout the record's retention period? *Yes, with proper archiving* - How can the audit trail be reviewed? *It can be reviewed on screen, exported to another file, or printed to paper.*
§11.10.e	Is the audit trail available for review and copying? *Yes*

21 CFR Part 11 Reference[1]	***Question***
§11.10.f	Only to be answered if applicable. If the sequence of system steps or events is important, is this enforced by the system? *Yes, where needed* - Are there sequences of operations, or sequential events, or sequential data entry, that is important to this system? If so, what are they? *Most activities require a sequence of commands (creating, running, etc.)* - If so, how does the system ensure that steps are followed in the correct sequence? *System / Application defined sequences cannot be edited / altered by user.*
§11.10.g	Are authority checks in place to ensure that only authorized individuals can use the system, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations? This requirement refers to functional access once a user logs into the system. *Yes* - Are there different levels of access based on user responsibilities? If so, what are they? *Yes, multiple authorization levels configurable by admin user.*
§11.10.h	Only to be answered if applicable. Does the system check the validity of the source of any data input or operational instructions? *Yes* - Are any devices used as sources of data? *No (only instrument)* - Are commands sent from a specific location e.g. via remote radio data terminals? *Commands are sent via USB cable from the PC to the instrument.*
§11.10.i	Is there evidence that system developers are competent to perform their assigned tasks (e.g. CVs, training records)? *Available via audit* - For vendor personnel, are there job descriptions, training records, and a training procedure that is followed? *Available via audit* - For the vendor's external (i.e., contract) personnel, are there resumes, training files or other written documentation of education, training & experience? *Available via audit* - What evidence exists of suitable qualifications and/or proficiency for developers and support personnel? *Available via audit* - Is there any system training for developers and/or support staff? *Available via audit*
§11.50.a	Do signed electronic records contain the printed name of the signer? *Yes* - UserID and full name of the signer are required? *Yes*
§11.50.a	Do signed electronic records contain the date and time of signing? *Yes* - What is the precision of time stamp (seconds, minutes)? *Seconds* - What is the source of the date & time stamp? *Computer date/time.*
§11.50.a	Do signed electronic records contain the meaning of the signing (e.g. approval, review, responsibility etc)? *Yes* - Is the meaning free format or pre-defined within the system? *Pre-defined & user configurable, optional user comments*

***21 CFR Part 11 Reference*[1]**	***Question***
§11.50.b	Is the following information shown whenever the signed electronic record is displayed? - printed name of the signer - Full name not user id must be displayed *Yes* - date and time of signing *Yes* - meaning of the signing *Yes*
§11.50.b	Is the following information shown whenever the electronic record is printed? - printed name of the signer - Full name not user id must be printed *Yes* - date and time of signing *Yes* - meaning of the signing *Yes* - Is the above information printed on ad hoc reports and queries also *Yes*
§11.70	Are electronic signatures linked to their respective electronic records? *Yes. The electronic signature is a permanent part of the data record in the database.* - Are signatures prevented from being excised, copied, or otherwise transferred to falsify an electronic record? *Yes*
§11.100.a	What system controls are in place to ensure electronic signatures are unique to an individual? *All User IDs must be unique – all past IDs are stored.* - Is there any documentation to show that individuals understand that electronic signatures are legally binding? *User responsibility*
§11.100.a	Can electronic signatures ever be reused by, or reassigned to, anyone other than the original user? *No*
§11.200.a.1 .i	Is the signature made up of at least two components, such as an identification code and a password? *Yes* - The id code/password combination must be unique. *Yes*
§11.200.a.1 .ii	When several signings are made during a continuous session, is the password executed with each signing? (Both components must be executed at the first signing of a session.) *Yes*
§11.200.a.1 .ii	If signings are not done in a continuous session does the system ensure that both components of the electronic signature are executed with each signing? *Yes (Signatures with both components are required where prompted at the time of operation)* - Does the system log-out after a period of inactivity? *No*
§11.200.a.3	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals? *Yes* - Could one person working alone forge another person's electronic signature? *No*

21 CFR Part 11 Reference	***Question***
§11.300.a	Are system controls in place to maintain the uniqueness of each combined identification code and password? *Yes* - Is uniqueness maintained historically? *Yes* - Does the system check for duplicate ids? *Yes* - Is the user forced to change a 'default' password immediately upon login? *Yes via User configurable option*
§11.300.b	Do passwords periodically expire and have to be revised? *Yes* - Does the system include functionality that requires users to periodically change their passwords? *Yes via User configurable option*
§11.300.d	Does the system take preventative measures once attempted unauthorized access attempts have been detected? *Yes* - Are 'attempts at unauthorised use' defined? *Yes* - Is the user locked out after unsuccessful access attempts? *Yes*
§11.300.d	Does the system provide notification of attempted unauthorized access? *Yes* - Does the system automatically report, log or send an e-mail to the system administrator? *Yes, via audit trail log* - Is an alarm function triggered? *No, except as described above. However, the user account is locked pending administrative investigation and release.*

conclusion

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 DataPro2 Software. 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. Sievers encourages everyone to be engaged in the conversation and ongoing interpretation. For more information about how the M9 TOC Analyzer and DataPro2 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.

References

1. CFR - Code of Federal Regulations Title 21. Retrieved January 16, 2018, from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFR-Search.cfm?CFRPart=11