SCIEX OS LC/MS Software and 21 CFR Part 11 Regulations

Author: Blair C. James

Purpose

The purpose of this paper is to present an approach to assist the user in achieving 21 CFR Part 11 compliance with SCIEX OS LC/MS software version 1.4 and above, when used for quantitative analyses supporting Good Laboratory Practice (GLP) bioanalytical studies. In this paper, we outline the joint responsibilities between a supplier and its customers to support users' 21 CFR Part 11 compliance. We hope you find the information both helpful and educational.

Introduction

21 CFR Part 11 is a US Food and Drug Administration (FDA) regulation that covers the trustworthiness and reliability of electronic records and electronic signatures. The regulation has been effective since August 20, 1997 and has since been reviewed and supplemented with additional guidance. On February 20, 2003, the agency issued a draft Guidance for Industry on Part 11 Scope and Applicability and, after a 60-day industry comment period, issued the final version on September 3, 2003.[2] This paper incorporates content from both the initial regulation and the final version of the Guidance for Industry. In April, 2016, the FDA issued a draft of "Data Integrity and Compliance with cGMP Guidance for Industry." The data integrity guidance is organized as a series of questions and answers and is helpful when interpreting 21 CFR Part 11 in the context of modern computerized systems. This paper is not intended to provide legal advice or interpret the law. For a complete statement of terms, reference should be made to the regulation and the complete Guidance for Industry.

Contents

We will discuss the following issues of 21 CFR Part 11 and how SCIEX OS can be configured to help meet the regulatory requirements associated with the underlying GLP predicate rule (21 CFR Part 58).

- What is 21 CFR Part 11? A brief history and current status of the regulation
- Discussion of open and closed systems in the context of SCIEX OS
- Definition of electronic records and how this is interpreted for SCIEX OS
- Controls required for 21 CFR Part 11: technical, administrative and procedural
- Impact of predicate rules for the interpretation of Part 11
- Roles and responsibilities for 21 CFR Part 11 compliance: the importance of partnership between the customer and the supplier
- Detailed discussion of 21 CFR Part 11 and certain responsibilities for each section in the regulation

What is 21 CFR Part 11?

An important driver for the "Electronic Records; Electronic Signatures" Final Rule[1] was the pharmaceutical industry, who approached the FDA with a request to use electronic records so that the industry could take advantage of modern technology and reduce the use of paper. Following the publication of a draft of the regulation in 1994, the final rule was published on March 20, 1997, and became effective on August 20, 1997.

In essence, the regulation provides the basis for the use of electronic records in place of paper records as well as the use of electronic, rather than handwritten signatures. Under 21 CFR Part 11, electronic records can be equivalent to the paper records required by predicate regulations (e.g. 21 CFR Part 58, the Good Laboratory Regulations).[3] Electronic signatures can be considered as legal equivalents to handwritten signatures. The regulation further stipulates that both electronic signatures and electronic records must be trustworthy and reliable.

The regulation impacts almost all FDA-regulated work (e.g. pharmaceuticals, medical devices, blood banks, food). It impacts bioanalysis directly when studies are used to support new drug applications or new formulations of existing drugs. Any organization that wishes to register products for sale in the USA, regardless of where the organization is based, must comply with the requirements of this regulation.

Key Requirements of 21 CFR Part 11

A summary of significant requirements of the regulation appears below. For more detailed explanations, including roles and responsibilities, please see the later sections of this paper. Please refer to the regulations themselves for a complete statement of these requirements.

Electronic Records

Electronic records (covered by Part B of the regulation) generated by any computerized system must be trustworthy and reliable. A number of controls are specified in the regulation to support this requirement.

- Systems must be validated
- Systems must be able to detect altered and invalid records
- Only authorized individuals must have access to a system and their access levels must align with their assigned responsibilities
- Audit trails are required to monitor creation of and changes to records, including archive or deletion of data
- People using a system must be trained; this includes all levels of support from system administration to front line users and IT support staff
- Records must be protected for the duration of the records retention period; this may be up to 15-20 years depending on the predicate rule, and for practical purposes can be considered to be permanent
- Systems must provide the data and associated meta data to an inspector if required
- Signing of records requires the name of the individual, reason for signing, and the date and time displayed at the time of signing

- Signatures must be linked to respective records so that the signatures cannot be removed or copied
- Policies must be established holding individuals accountable for actions taken under their electronic signatures
- Where data confidentiality is required, the addition of security such as file encryption or digital signatures is required to ensure confidentiality
- The system, including training and resultant records, must be sufficient to prevent repudiation of electronic signatures as not genuine

Electronic Signatures

Part C of the regulation has many requirements for procedural and administrative controls, with relatively few technical requirements. While the use of electronic signatures is voluntary, and each company can choose to implement electronic signatures or not, there are also pertinent security requirements for the trustworthiness and reliability of electronic records; for example, the ability to detect unauthorized access to a system in §11.300(d).

The main requirements are:

- Individuals using electronic signatures must have their identities verified
- Companies must send a letter to the FDA certifying that when electronic signatures are used, they are the legal equivalent of traditional handwritten signatures
- Electronic signatures must be unique to an individual and never reused by a company
- Controls must be in place to prevent fraud (Fraud would require the collaboration of two or more individuals)
- The system must be able to detect attempts of unauthorized access and notify the appropriate security/management staff

Impact of the Part 11 Scope and Applicability Guidance

Since 2002, the FDA has been re-evaluating the Good Manufacturing Practice (GMP) regulations and as part of this program,[2] five key sections of the Part 11 regulation include enforcement discretion (Table 1).

For example:

Validation of Part 11 requirements

- Copies of records
- Records retention
- Audit trail
- Legacy systems (i.e., systems already in operation before August 20, 1997) do not need to comply with 21 CFR Part 11 regulations, provided they were validated to meet the applicable predicate rule requirements before Part 11 was in effect and any changes do not invalidate their ability to meet predicate rule requirements.

Part 11 Requirements Still Enforced	Part 11 Requirements with Enforcement Discretion
11.10(d) Limiting system access to authorized individuals	11.10(a) Validation
11.10(f) Use of operational system checks	11.10(b) Copies of records
11.10(g) Use of authority checks	11.10(c) Record Retention
11.10(h) Use of device checks	11.10(e) Audit trail
11.10(i) Persons… have the education, training, and experience to perform their assigned tasks	Legacy Systems operating before August 20, 1997
11.10(j) Written policies that hold individuals accountable for actions	
11.10(k) Appropriate controls over systems documentation	
11.30 Controls for open systems	
11.50 Signature manifestations	
11.70 Signature / record linking	
11.100 General requirements	
11.200 Electronic signature components and controls	
11.300 Controls for identification codes/passwords	

Table 1. Enforcement discretion. Note that the remainder of 21 CFR Part 11 is still in operation and will be enforced by the FDA as shown in this table.

Impact of 21 CFR Part 11 on Bioanalytical Laboratories

When the regulation became effective, no LC/MS systems operating in bioanalytical laboratories were fully compliant with the requirements. Typical problems included:

- No audit trail—only a history log in the data file
- Little or no security (security features if available were difficult to use efficiently and effectively)
- File overwriting, with or without warning
- Changes of data could be made with no record of the original value
- No electronic signatures (while not a compliance problem, per se, this impaired the usefulness and benefit of an electronic system)

LC/MS instruments were used as hybrid systems; meaning that although they generated electronic records, handwritten signatures were applied to paper copies of the records.

Key Part 11 Definitions Explained

Open and closed systems

21 CFR Part 11 classifies computerized systems as either "open" or "closed" in Part A (Scope section); there are only two words of difference between the two definitions (in parentheses below):

Closed (Open) system means an environment in which system access is (not) controlled by persons who are responsible for the content of electronic records that are on the system.

The key points of this definition are:

- The regulation refers to a "system," an application is not mentioned; in fact, there is no place in the regulation that mentions application. "System" includes hardware, software, people, training policies, etc.
- "System" is given a wide definition, and includes the information technology (IT) network that traditionally was not included in regulatory inspections prior to the issuance of 21 CFR Part 11

SCIEX OS is Designed for Closed Systems

Current SCIEX OS software can be used in either a closed or open system. However, it can be configured to support compliance only in a closed system. It can be used within an organization either as a standalone or single system (Figure 1) or in a networked configuration (Figure 2) where multiple acquisition workstations and data processing stations may be connected to a closed network. For the rest of this paper, we will only consider closed systems.

SCIEX OS organizes and stores its data in a "root directory", located on the local acquisition workstation hard drive. Workstations hosting SCIEX OS may be connected to a network, and utilize the network's user management and credentials verification, but the root directory should not be located on a network drive. When processing (quantifying) data, SCIEX OS has the ability to open a raw data file from any visible storage location.

Standalone or single systems?

One or several standalone SCIEX OS systems in a bioanalytical laboratory are closed systems. The facility will have physical security and there will be logical security to prevent unauthorized persons from gaining access to the application.

Standalone workstations (or network computers, for that matter) that hold electronic records present the risk of disk failure or corruption of records and require regular backups to support preservation of the electronic records.

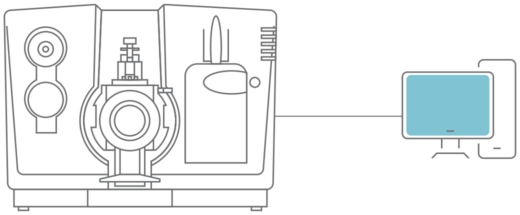

Figure 1. Standalone SCIEX OS software systems in a laboratory.

Networked Systems

To assist in managing user credentials, SCIEX OS may be connected to a Microsoft Windows Active Directory network. It is important to note that the networking of several SCIEX OS systems supported by an IT department does not mean that the system is now open. Interpretation of "environment" needs to be wider than just the laboratory, and encompasses the wider organization, including controlled network objects such as network data storage locations and data transmission lines. Whether standalone or connected to a network, SCIEX OS systems must have written procedures and documented evidence that protection of records (backup) is undertaken regularly and reliably.

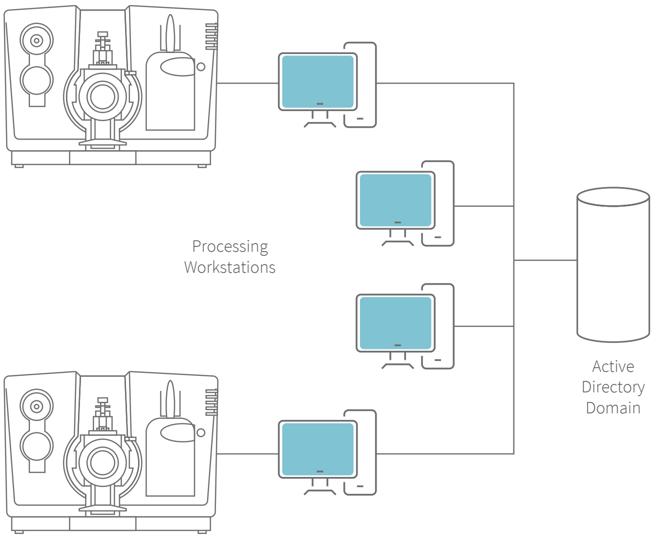

Figure 2. Networked SCIEX OS software LC/MS systems with the Active Directory network managing user credentials.

Electronic Records

"Electronic record" is defined in the regulation:

Electronic Record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.[1]

This is a very broad definition. The phrase "other information representation" covers any electronic record in any format.

The Guidance on Part 11 Scope and Application 2 narrows the scope of the regulation in certain circumstances. It still allows the use of paper records, if the paper output meets the requirements of the applicable predicate rules. It is often not practical to define the paper records for the raw data output of SCIEX OS due to the number and volume of records that the software generates with each run. In the context of SCIEX OS, the electronic records produced during a bioanalytical run consist of the LC/MS raw data:

- LC/MS data files – single sample in a single WIFF file, multiple samples within a single WIFF, combinations of multiple samples, and multiple WIFF files
- Quantitation results tables including the audit trail incorporated with each results table
- Processed data file(s)
- Audit trails and history logs

The contents of the following types of files are copied to and stored with the associated raw data file:

- Acquisition method file
- Processing method file
- Hardware configuration profile
- Tuning and instrument parameter settings

The above records may be stored and archived with the associated data files but are not strictly necessary because the data files themselves contain the same information (metadata) as stored in these files.

To help ensure the trustworthiness and reliability of electronic records, each file produced by the system must have the means to be uniquely identified. Therefore, a file naming convention and SOP is strongly advised to prevent file overwrites by administrators or inadvertent appending of samples into the wrong data file. SCIEX OS provides automatic increment of batch and method names for all regular users (administrators may overwrite methods but the default configuration requires a signature for the overwriting of the method/batch).
Note that sample data within a WIFF file pair collected under a specific method retains the original method information with the sample data. SCIEX OS automatically appends data files with new samples; original data are not overwritten.

Electronic Signature

"Electronic signature" means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.[1]

Electronic signatures that can be used under Part 11 are one of the following three types:

- Electronic signature (password and user ID (identification code which may or may not have elements of the user's actual name)). This is the easiest method to implement in many applications used in bioanalysis, but its effectiveness is highly dependent upon the quality of the password chosen by the user. Passwords that are easily remembered can often be easily guessed; this is the so-called password paradox.
  - There has been debate on the effectiveness of various password policies. Long complex passwords and frequent changes to passwords results in people writing passwords down or cycling through passwords. A full discussion of cyber-security principles is beyond the scope of this paper, but the current Microsoft Password Guidance document (https://www.microsoft.com/en-us/research/publication/password-guidance/) offers the following advice:
    - › Maintain an 8-character minimum length requirement (and longer is not necessarily better)
    - › Eliminate character-composition requirements
    - › Eliminate mandatory periodic password resets for user accounts
    - › Ban common passwords, to keep the most vulnerable passwords out of your system
    - › Educate your users not to re-use their password for non-work-related purposes
    - › Enforce registration for multi-factor authentication
    - › Enable risk based multi-factor authentication challenges
- Biometric signature (based on a measurable human trait such as fingerprint or iris recognition). The prices of fingerprint devices are dropping to reasonable levels and multi-mode verification devices (verifies print + temperature + pulse etc.) are more difficult to fool and becoming readily available. However, the use of fingerprint technology in a bioanalytical laboratory may be hampered by the need to use gloves for many bioanalytical activities.
- Digital signature (public/private key infrastructure plus a personal pass-phrase or password). Implementing digital signatures usually requires a token or equivalent that generates a random number that is synchronized with the same algorithm running with the application.

SCIEX OS relies on the implementation of electronic signatures comprised of user identity and password. SCIEX OS security works in conjunction with Microsoft Windows security, authenticating against network User IDs and passwords or local User IDs and passwords.

The customer must administer passwords through the use of SOPs, training, and tools to ensure that:

a. The user IDs and user names are unique and never reused

b. Passwords are suitably secure, strong passwords, known only to their user

c. The user ID/password combination is used only by its respective owner

The Role of the Predicate Rule in Part 11 Interpretation

Part 11 has always been interpreted using the existing predicate rules. The predicate rule interpretation has been emphasized in the 2003 Guidance for Industry[2] to ensure that a practical scope of Part 11 is made during the review period.

For bioanalysis, the main predicate rule regulation is 21 CFR Part 583 (Good Laboratory Practice), although 21 CFR Part 320 (the bioavailability regulations) may also apply. However, 21 CFR Part 11 makes no mention of which records must be generated, signed and maintained; this is determined by the applicable predicate rule(s).

The predicate rule will state those records that are required, and those records requiring signature. Where the predicate rule requires a record, Part 11 says you may use an electronic record. Where the predicate rule requires a signature, Part 11 says you may use an electronic signature. Where the predicate rule does not identify a record or a signature as required, Part 11 requirements do not apply (note that there are records identified specifically in 21 CFR Part 11, such as audit trails, that may not have a direct paper equivalent).

However, bioanalysts working in the pharmaceutical industry or contract research organizations often generate paper and sign records regardless of what is actually required by the predicate rules. When implementing ER/ES systems, it is important to understand exactly what signing actions are required and where it is important to identify an individual's actions. For example, when you make a handwritten change to a worksheet, is a full signature required or just initials? This is an important distinction to make and understand. What is the role of the signature or initials? Is it the identification of an individual that denotes who performed an action, or is it the approval or authorization of results or a report?

This is a critical issue, as the implementation of many data systems and LIMS used in bioanalysis can have an "electronic signature" associated with writing to the database. In fact, per the applicable predicate rule, the signing requirements are very limited. However, in many labs it is still the practice to sign and date virtually every scrap of paper.

Interpretation of Part 11 by the GLP Predicate Rule

To illustrate the need to understand and correctly interpret the predicate rule, we will first present the predicate rule for equipment design, and then highlight key issues.

21 CFR Part 58.61: Equipment Design[3]

The requirement for equipment design under the GLP predicate rule states:

Equipment used in the generation, measurement, or assessment of data and equipment used for facility environmental control shall be of appropriate design and adequate capacity to function according to the protocol and shall be suitably located for operation, inspection, cleaning and maintenance.

Some of the key elements of this predicate rule requirement for SCIEX OS and SCIEX mass spectrometers that they control are as follows:

- Appropriate design – Validation of the system, including instrument qualification; specify the intended use of the instrument and software and test against the requirements
- Adequate capacity – Part of the specification and testing during the validation must cover the expected uses of the system such as the ability to control the applicable instrumentation hardware, to collect the necessary data for a given sample, to run up to the protocol's maximum number of analytical samples and injections, to report the data, and to store the data collected. The storage capacity of the LC/MS data storage location must be evaluated for suitability.
- Suitably located – Location must meet the manufacturer's specifications for physical location/ambient conditions, and provide the services required for effective operation such as electricity and gas supplies
- Maintained – Service and maintenance history for the instrument and software must be provided

Risk Analysis to Determine the Extent of Validation

As the FDA Guidance on Part 11 Scope and Application[2] states:

We recommend that you base your approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.

An important issue is to understand how the LC/MS instrument and SCIEX OS subsystems affect the product quality. This can mean quality of the manufactured drug product and could also be interpreted as the quality of the data generated and subsequently included in bioanalytical reports. Therefore, in the context of SCIEX OS, it is the quality of the data generated by the bioanalytical laboratory.

Another issue is: Where does the system fit into the development pipeline?

- Late research to identify potential development candidates
- Non-clinical development
- Clinical development

The later in development the system is used, the greater the risk, as the data is used for pharmacokinetic interpretation, bioequivalence studies, etc. There is also a greater possibility that the data will be included in regulatory submissions. If used for two or more development phases, then the extent of validation should be based on the risk in each of the areas of use.

Roles and Responsibilities Involved in 21 CFR Part 11

In this section, we will discuss the nature of the Part 11 controls and who is responsible for each (Figure 3).

Three Types of Part 11 Controls

21 CFR Part 11 requirements can be classified into one of three types of control:

- Administrative Controls – These are policies for 21 CFR Part 11 within an organization and can include a company interpretation of the regulation and how the company will verify the identity of individuals, and ensure non-repudiation of electronic signatures
- Procedural Controls – These are essentially standard operating procedures (SOPs) or other written instructions for a system, including how to use the system (this may require two SOPs, one for the system administrator, and one for the users), a list of authorized users against access level (which is reviewed periodically to confirm that it is correct), and backup and recovery procedures
- Technical Controls – Examples of technical controls are the security and access control for the application and the audit trail to monitor changes to the records

Note: you cannot be compliant with Part 11 until all three types of controls have been implemented. The number and extent of the controls required for SCIEX OS will depend on how the system will be used. For example, when SCIEX OS is used as a hybrid system, which appears acceptable to the FDA under the Scope and Applicability guidance, then fewer technical controls are required compared with when it is used with electronic signatures.

Interrelationships Between Technical and Procedural Controls

Some technical controls do not stand on their own. They require a procedure to ensure that they are implemented and are effective.

Examples include:

- 11.300(d) The system must have the ability to detect unauthorized use; the host operating system (Windows, or Active Directory) is responsible for controlling access, and must be configured appropriately, including to record and report unauthorized access attempts.
- 11.10(d) limits system access to authorized individuals and 11.10(g) requires authority checks to ensure that people only have access to functions appropriate to their position and training. A SOP must be in place for defining and implementing these two requirements, and also listing the authorized users and their individual access levels

Likewise, administrative and procedural controls are not sufficient, by themselves, when a technical control is available. For administrative and procedural controls to be effective, the human components of the system must function perfectly, which is rarely the case, so available technical controls should always be utilized.

We will look at this in more detail in the pages that follow, as we review the requirements for 21 CFR Part 11.

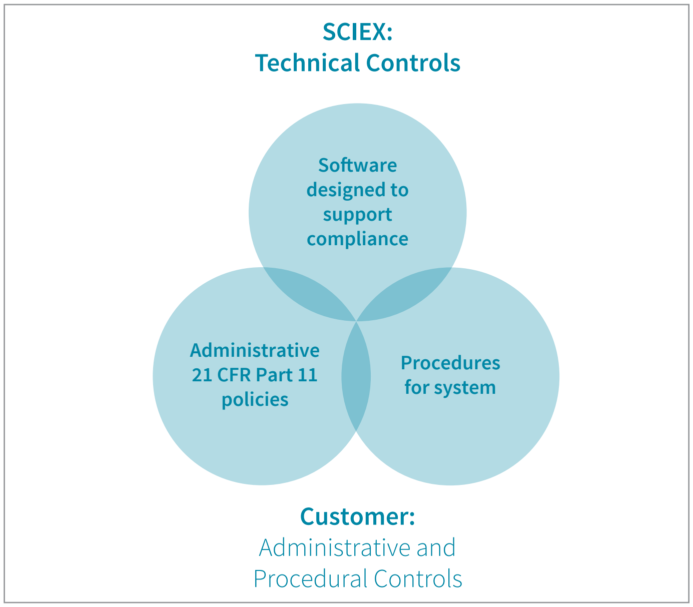
SCIEX:
Technical Controls
Software designed to support compliance
Administrative 21 CFR Part 11 policies
Procedures for system
Customer:
Administrative and Procedural Controls

Figure 3. Three types of controls required for 21 CFR Part 11 compliance.

Partnership for Part 11 Compliance

It is important to note that you cannot buy a “21 CFR Part 11-compliant” system. There are applications, such as SCIEX OS, that can be designed as 21 CFR Part 11-ready, but it is the user who is responsible for appropriate configuration of SCIEX OS and supporting network/ Windows system security, as well as for providing policies, procedures, and user training to ensure the systems are fully compliant with the applicable regulations.

SCIEX OS Features Supporting 21 CFR Part 11 Implementation and Responsibilities of Customer for Implementation

*Note that only versions of SCIEX OS version 1.4 and greater have the 21 CFR Part 11 supporting features.

§11.10 Controls for Closed Systems

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
a. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	• Provide applicable features to detect changes to electronic records • Detect corrupted data files • All alterations automatically recorded in an audit trail at time of saving • Development of the software under a quality management system	• Responsible for initial instrument qualification and software validation • Responsible to maintain the validated state via the change control procedure • Write, maintain, enforce relevant SOPs
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	• Execution of signature, audit trail and all supporting information must be linkable to results • Provision of printing and export to PDF file format features	• Configure the OS and SCIEX OS to prevent deletion or unauthorized copying of files through the operating system • Control the date and time settings on the workstation
c. Protection of records to enable their accurate and ready retrieval throughout the records retention period	• Future software upgrades must be backward compatible with existing files and data or provide translation to new format • Multiple users must not be allowed concurrent access to the same record	• Define record retention period • Write SOPs for backup, recovery, archive and restore • Identify and deploy any additional software tools necessary for this operation
d. Limiting system access to authorized individuals	• Software provides means to limit access to application via a unique User ID/password • Software prevents the viewing or copying of passwords • Software provides logs of security access and changes to security settings	• SOP on System Security and Access Control must cover the proper configuration and maintenance of Windows user IDs and passwords • List of current and historical users with access privileges • Enable security features in SCIEX OS. • Use Windows screen saver and lockout.
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. Recorded 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	• Audit trail for application and system events • Automatic version control to capture content changes • Non-editable audit trail that can only be searched, viewed and printed	• Enable audit trail on installation • SOPs to reflect the retention of records including the corresponding audit trails
f. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	• Built into application	• Windows screen saver Inactivity lockout must be enabled in the operating system
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	• Software provides ability to define individual user permissions • Software allows updates to access rules only through validated secure application screens • Software provides means of authenticating user accessing the application or conducting specific operations within the application	• SOP on System Security and Access Control • Configure Windows® security on computers • Configure user access to component features within SCIEX OS • Enable electronic signature features
h. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction	• Built into application • Status polling of instrumentation • Confirmation of methods against instruments attached	• SOP to cover operation of LC/MS equipment
i. Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks	• SCIEX software development quality system • Documented training records	• Vendor audit or checklist • Signed training records for system users and maintenance staff
j. 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	• Not applicable	• Notify FDA of intent to use signatures • SOP on non-repudiation of electronic signatures

k. Use of appropriate controls over systems documentation including: 1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	• Link system documentation to a specific release of software • Software provides audit trail for maintenance activities on the instrument	• SOP on Change Control • Retention of records dealing with instrument maintenance as part of system maintenance under predicate rules for equipment maintenance • SOP on System Security and Access Control • Version control on all documents

§11.50 Signature Manifestations

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
a. Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 1. The printed name of the signer; 2. The date and time when the signature was executed; and 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature	• Software displays the full name of the user on screen at the time of signing • Provision of audit trail linked to the signed records with provisions for items (1), (2) and (3) • Software allows the creation of specific meaning for the signature with the use of the configurable reason options	• SOPs governing user account setup include the input of the person's full name. List of full names to ensure that name is not duplicated (especially in larger companies) • Configure and document the allowable meanings of signatures in the 'reason' dropdown option
b. 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 record (such as electronic display or printout)	• Software provides links through the audit trail that link the records to the signature execution/ authentication	• Customer must view and print separately the audit trial manifestation of e-signatures as the record of the e-signature on the applicable electronic records

§11.70 Record and Signature Linking

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
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	• Software records signing event in the audit trail and provides linkage to the applicable record • Software to prevent a reasonable attempt to excise an electronic signature and apply it to another record	• SOP for signing electronic records • Handwritten signatures on electronic records must be cross referenced to the signed records • Applicable audit trail manifestations of electronic signatures and history of the specific record may need to be printed

§11.100 General Requirements

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
a. Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	• Not applicable	• SOP on System Security and Access Control • Proper configuration of user accounts under Windows® Security (list of User IDs to prevent reissue or reuse of user ID • No shared user accounts permitted
b. 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	• Not applicable	• SOP for verifying an individual's identity
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 1. 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	• Not applicable	• Pharmaceutical company or CRO sends a letter to the FDA

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	• Not applicable	• SOP on FDA Inspections
2. 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	• Not applicable	• SOP on FDA Inspections

§11.200 Electronic Signature Components and Controls

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
a. Electronic signatures that are not based upon biometrics shall: 1. Employ at least two distinct identification components such as an identification code and password	• Application uses Windows® Security as source of user identity and password used as electronic signature components	• SOPs identified in previous sections
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	• SCIEX OS provides means to enter user identity and password for initial log into application • SCIEX OS allows a user while in a continuous period of controlled access to input their password only for subsequent signings (user ID is provided automatically) • Windows monitors activity and locks out user (ends the session of continuous access) if no user activity is detected	• SOP on System Security and Access Control • Enable Windows screen saver with lockout.
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	• SCIEX OS provides means to enter user identity and password for first signing of each continuous period	• SOP on System Security and Access Control • Enable Windows screen saver with lockout.
1. Be used only by their genuine owners; and	• SCIEX OS authenticates user credentials against Windows Security and verifies user identity against list of allowed users in application	• SOPs identified in previous sections • Each user identity is unique and never reused
2. 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	• SCIEX OS does not present passwords on the screen • SCIEX OS prevents the excising of passwords by normal means from fields on screen	• SOPs around User ID Password Administration issue, locking of accounts, etc.
b. Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	• Not applicable as biometrics are not used in SCIEX OS	• Not applicable

§11.300 Controls for Identification Codes and 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:

21 CFR Part 11 Regulation	SCIEX OS Software*	SCIEX OS Software Customer
a. Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password	• SCIEX OS provides the ability to show current security configuration with applicable user IDs, and ability to print or show history of security including the addition and deletion of users	• Ensure user identities are never reused • Maintain historical list of User IDs and User Names from Windows® Security • Maintain history of security changes or Windows settings • Maintain list of application security changes (SCIEX OS Audit Trail)
b. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)	• SCIEX OS retains log of system access events	• Establish and enforce password policy • SOP on System Security and Access Control: review the list of users • SOP for the periodic review of system access logs against list of users

c. Following loss management procedures to 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	• Not applicable	• SOP on System Security and Access Control
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	• SCIEX OS generates entry into audit trail • Windows provides lock out, log off feature	• Enable Windows screen saver inactivity lockout • On the operating system, account policies enable automatic lockout if permitted number of failed attempts is exceeded
e. 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	• Not applicable to SCIEX OS	• Not applicable

Final Considerations

Moving from Paper to Electronic Records

Working electronically requires a change in mindset. The concepts of “raw data” and “derived data” now become simply electronic records—and all must be retained and protected for the records retention period. Electronic records for a chromatography data system or mass spectrometry data system, for example, consist of the actual observed values (for a MS or HPLC run this would be the electronic data file) plus the associated electronic records to interpret the data file such as:

- Method parameters
- Instrument parameters
- Sequence data
- Integration parameters
- Calibration method and results
- Audit trail

SCIEX OS simplifies the management of electronic records by embedding relevant metadata in the actual data file. Still, the extent of electronic records is much greater than paper, which is a tangible medium, but electronic records are not and can be difficult to visualize.

It bears repeating that SCIEX OS is inherently an electronic records application. Raw electronic data files (such as the WIFF files and result table files) must be protected and retained if the contents of those files are later printed and treated as non-electronic records.

Benefits of 21 CFR Part 11

Process redesign is essential in order for business to fully realize the benefits of 21 CFR Part 11, but the benefits of working electronically can be considerable, including significant cost and time savings, as well as overall process improvement, and a faster, smoother path to regulatory approval. Some of the savings that can be realized are based upon the following activities:

- Eliminating paper
- Reducing number of applications to validate
- Eliminating manual involvement and speeding up the process; e.g., tasks such as typing data into systems, followed by manual verification to identify transcription errors
- Eliminating redundant tasks from the process to reduce the overall time for process execution

References

1. U.S. Food and Drug Administration Federal Register 1997, 62, 13430-13466

   Regulation Portion:

   Department of Health and Human Services, Food and Drug Administration 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule March 20, 1997 Federal Register/Vol. 62, No. 54/Thursday, March 20, 1997/ Rules and Regulations 13464-13466

2. U.S. Food and Drug Administration Guidance for Industry:
   21 CFR Part 11; Electronic Records; Electronic Signatures Part 11 Scope and Application, 2003

   i. Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application (DRAFT GUIDANCE) February 20, 2003

   ii. Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application, August 28, 2003

3. U.S. Food and Drug Administration Federal Register 1978, 43, 59986-60020

   Regulation Portion:

   Department of Health, Education and Welfare, Food and Drug Administration 21 CFR Part 58 Good Laboratory Practice for Nonclinical Laboratory Studies December 22, 1978 60013–60020

   Amendment to 21 CFR Part 58:

   Department of Health and Human Services, Food and Drug Administration 21 CFR Part 58 Good Laboratory Practice Regulations Final Rule, September 4, 1987 Federal Register/Vol. 52, No. 172/ Friday, September 4, 1987/Rules and Regulations 33768- 33782

Headquarters
500 Old Connecticut Path
Framingham, MA 01701 USA
Phone 508-383-7700
sciex.com

International Sales
For our office locations please
call the division headquarters or
refer to our website at
sciex.com/offices

SCIEX
The Power of Precision