White Paper

Agilent
Trusted Answers

Support for Title 21 CFR Part 11 and Annex 11 compliance: Agilent Fragment Analyzer systems, valid for Fragment Analyzer Controller 5.0.0 Software and ProSize Data Analysis 6.0.0 and Security Module

Overview

US FDA Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its EU analog, Eudralex Chapter 4, Annex 11, describe the requirements for electronic records and electronic signatures for regulated pharmaceutical and Biopharmaceutical organizations.

21 CFR Part 11 was first written into law in 1997 and subsequently updated in 2003. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with integrity.

This white paper is a resource for users of Agilent Fragment Analyzer systems whose organizations must comply with these regulations. The Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software 6.0.0 Security Module controls acquisition and processing of Fragment Analyzer data. It is the responsibility of the user and their organization to ensure that the functionalities provided by the Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software 6.0.0 Security Module are used appropriately to ensure compliant operation for laboratory data acquisition and processing. In addition to the technical controls the Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software 6.0.0 Security Module provides, the user organization must establish procedural controls–standard operating procedures (SOPs)– to address relevant non-technical requirements and to fill gaps that are not provided from the software feature set. For example, controls such as internal audit programs, must also be established to ensure that system operators follow the SOPs.

Appendix 1 provides a detailed description of how Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software 6.0.0 Security Module supports users and their organizations in fulfilling the requirements of each section of 21 CFR Part 11 and the related sections of EU Annex 11. The descriptions assume that system access, including instrument hardware and software, is controlled by the staff responsible for the electronic records contained on the system. Thus, the system is designed as a “closed system” as defined in 21 CFR Part 11.3(b)(4).

21 CFR Part 11

21 CFR Part 11 covers three specific elements of a regulated laboratory's operation:

– Security of electronic records,

– Attribution of work,

– Electronic signatures (if used)

Security

As per ISO/IEC 17799, also known as ISO/IEC 27002, security can be interpreted as "the right people, having the right access, to the right information." Regulated organizations must be able to both verify the identity of system users and limit system access to trained, authorized individuals (11.10(d), (i) and (g); 11.100(b)). Because laboratory staff have different responsibilities based on their job assignments, data access and controls must be segregated to make sure that they can perform only allowed operations on data records that are required to fulfill their responsibilities.

Attribution of work

Attribution of work refers to documenting the "Who, what, when, where and why?" of work performed. Automated audit trails independently record users' actions thus connecting laboratory staff to the work they perform. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

– *Who:* clearly identifies the person responsible for the particular action that creates, modifies, or deletes a record.

– *What:* is the action that took place, including, if applicable, the old value and the new value contained in the record.

– *When:* unambiguously declares the date and time the action took place.

– Where: clearly identifies the impacted record.

– *Why:* explains the reason for a change to a regulated record. The reason is often selected from a list of pre-defined reasons to provide consistency and to enable searching and sorting of entries.

eSignatures

While 21 CFR Part 11 does not require the use of eSignatures, it does provide regulations for their use when they are used. In this case, the system must ensure that eSignatures:

– Are irrevocably linked to their respective records.

– Show the full name of the signer, date and time, as well as the meaning of, or reason for, the signature (such as review, approval, responsibility, or authorship).

– Are present whenever the signed records are displayed or printed.

Topology

The Fragment Analyzer Controller Software 5.0.0 and ProSize Data Analysis Software 6.0.0 Security Module operate as a workstation.
The workstation allows direct control of an instrument from a standalone PC (desktop), with all data stored locally as a file-based system. This software release does not support client-server.

Compatibility

Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software rev. 6.0.0. Security Module is not compatible with previous software release.

"Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users."

– **Botha, Eloff,**
IBM Systems Journal[1]

1. Validation

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(a)	1.1 Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S.U	Required by all regulations. This is a typical example of shared responsibility between the system supplier and the user organization. While the user organization has ultimate responsibility for validation, some tasks can only be done and must be delivered by the software supplier, e.g., validation activities during development and related documentation. 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。	Partially Yes	Agilent Technologies has thoroughly tested the performance of the Fragment Analyzer Controller Software 5.0.0 and ProSize Data Analysis Software 6.0.0 Security Module to ensure accuracy, reliability, and consistent performance. This statement in no way releases the user organization from their regulatory responsibility to validate their analytical system in compliance with regulatory requirements and its intended use. To support with these regulatory requirements, Agilent offers IQ/OQ services for both hardware and software. For additional information about IQ/OQ services, please contact your local sales representative. With respect to Agilent Fragment Analyzer Controller Software Security Module, "regulated records" are: **Fragment Analyzer Controller Software** – Separation methods – Conditioning methods – Cleaning methods – Acquired data – Fragment Analyzer controller software associate events **ProSize Data Analysis Software** – Data analysis parameters – Data approval – Analysis results – ProSize data analysis software associate events – Result Reports **Administration Software** – Activity Log Additional details on “regulated records” can be found in the Fragment Analyzer software Security Module User documentation. The product does not come with a content management. It is User’s organization responsibility to maintain accuracy, reliability, and the ability to discern invalid or altered records. The Fragment Analyzer Software Security Module check-sums is available to detect/discover any “invalid or altered records” introduced during the time the software installer file is downloaded.
Annex 11	1.2 Is infrastructure qualified?	U	Annex 11. Principle B Brazil GMP 577	N/A	Qualification of infrastructures, such as servers and networks, is the responsibility of the user organization.

2. Accurate Copies and Secure Retention and Retrieval of Records

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(b)	2.1 Is the system capable of generating accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA?	S.U	第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （一）为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。	Yes	Records are available in both print and electronic formats, as PDF file from the Fragment Analyzer controller software. Records are available in both print and electronic formats, as a secured PDF file from ProSize data analysis software.
Annex 11	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	S	Annex 11.8.1 Brazil GMP 583		Records are available in both print and electronic formats, as PDF file from the Fragment Analyzer controller software. Records are available in both print and electronic formats, as a secured PDF file from ProSize data analysis software.
Brazil	2.3 Are their controls to ensure that the data backup, retrieval and maintenance process is duly carried out?	U	Brazil 585.2 第五 章系统 第十九条以电子数据为主数据时，应当满足以下要求： （三）应当建立数据备份与恢复的操作规 程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	No	The process of backing up data and maintaining data is responsibility of the user's organizations.
Part 11 11.10(c)	2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	U	China GMP 163	No	It is the user organization's responsibility to maintain the physical security of the raw data and result data generated by the Fragment Analyzer system. It is the user organization's responsibility to develop a review by exception protocol based on a risk-based assessment of unplanned events, such as instrument connectivity loss which would initiate a failover mode. It is the User's responsibility to implement security protocols around the folders where the data and reports are archived during the records retention period.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability, and integrity?	U	Annex 11.17	No	It is the responsibility of the user organization to ensure data are checked during archival for accessibility, readability, and integrity.

2. Accurate Copies and Secure Retention and Retrieval of Records continued

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Annex 11	2.6 If relevant changes are made to the system (e.g., computer equipment or programs), is then the ability to retrieve the data ensured and tested?	S.U	Annex 11.17	Yes	Fragment Analyzer controller Software 5.0.0 and ProSize data analysis software rev. 6.0.0 . Security Module is not compatible with previous software release. The data from earlier software release can be opened as read-only files. It is user's responsibility to ensure readability of the system's data during their implementation and validation processes.
Annex 11	2.7 Are data secured by both physical and electronic means against damage?	S.U	Annex 11.7.1 Brazil GMP 584 第五章系统 第十条系统应当安装在适当的位置，以防止外来因素干扰。 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如 计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。	Yes	The .psda files are acquired with the Fragment Analyzer controller software and stored on the workstation computer in a database file. Physical security is the responsibility of the user's organization. It is user's responsibility to provide a secured data storage location.
Annex 11	2.8 Does the system allow performing regular backups of all relevant data?	U	Annex 11.7.1 China GMP 163 Brazil GMP 585 21 CFR Part 211, 68 b	No	The process of backing up data is the responsibility of the user's organization.
Annex 11	2.9 Is the integrity and accuracy of backed-up data and the ability to restore the data, checked, validated, and monitored periodically?	U	Annex 11.7.2 China GMP 163 Brazil GMP 585 Part 211, 68 b	No	It is the responsibility of the user organization to ensure the integrity and accuracy of backed¬ up data, and to check, validate and monitor restored data periodically.

3. Authorized Access to Systems, Functions, and Data

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(d)	3.1 Is system access limited to authorized persons?	S.U	China GMP 183 163 Brazil GMP 579, ICH Q7.5.43	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. Duplication of the user ID is detected and prevented by the system. It is user's organization responsibility to clearly defined roles and responsibilities to prevent conflict of interest.
	3.2 Is each user clearly identified, e.g., through his/her/their own user ID and Password?	S.U	Several Warning Letters Please refer to US FDA Warning Letters for examples, and here is the link (Warning Letters | FDA) to search them.	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. Duplication of the user ID is detected and prevented by the system. It is user's organization responsibility to clearly defined roles and responsibilities to prevent conflict of interest.

4. Electronic Audit Trail

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(e)	4.1 Is there a secure, computer- generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records?	S.U	China GMP 163 第五章系统 第十六条计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改一个已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结 果，考虑在计算机化系统中建立一个数据审计跟踪系统，用于记录数据的输入和修改。	Yes	All user activities are recorded in secure, computer generated, time-stamped audit trails. Audit trails are created for all result data, methods, and configuration files.
FDA GLP	4.2 Does the audit trail record who has made which changes, when and why?	S.U	FDA 21 CFR P art 58.130 e	Yes	The audit trail includes the user ID, date and time of the change, and the before and after values. It is user's organization responsibility to record the reason for changes.
Annex 11	4.3 Can the system generate printouts indicating if any of the e-records have been changed since the original entry?	S	Annex 11, 8.2	Yes	Audit trails for records that include changes can be printed from any audit trail window.
FDA CGMP	4.4 Does the audit trail include any modifications to an established method employed in testing? 4.5 Do such records include the reason for the modification?	S	21 CFR Part 211.194 8b	Yes	Changes made to a method at run time will be saved in the data event log. Changes made to a method outside of run time, will result in a new method being created.

4. Electronic Audit Trail continued

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	S.U	Warning Letter Please refer to US FDA Warning Letters for examples, and here is the link (Warning Letters | FDA) to search them.	Yes	The system has a built-in Audit Trail within the application; however, it is the user organization's responsibility to enable it during installation. Once activated, the Audit Trail cannot be turned off or deactivated.
Annex 11	4.7 Is audit trail available in a generally intelligible form for regular review?	S	Annex 11, 9	Yes	The audit trail and activity log record all relevant entries in a chronological, human-readable, and easily understandable format. Users have the option to apply filters to find specific and meaningful activities.
	4.8 Can audit trail contents be configured such that only relevant activities are recorded for meaningful review of audit trail information?	S	Implicitly required by Annex 11 with many warning letters related to review of audit trails.	Yes	The audit trail and activity log record all relevant entries in a chronological, human-readable, and easily understandable format. Users have the option to apply filters to find specific and meaningful activities.
Part 11 11.10(e)	4.9 Is previously recorded information left unchanged when records are changed?	S		Yes	All system changes and modifications to electronic records are recorded in the audit trails and activity log. Any changes made to electronic records must be saved as a new individual file to ensure uniqueness and traceability. The system does not support version control.
Part 11 11.10(e)	4.10 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?	S.U		Yes	Measurement files that include audit trails are user organization's responsibility to maintain based upon their SOP retention period, and it is readily available to view and analyze.
Part 11 11.10(e)	4.11 Is audit trail available for review and copying by the FDA?	S		Yes	Audit trails can be viewed and printed in a PDF format.
Annex 11	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?)	S	Annex 11, 8.1	Yes	Audit trails can be viewed and printed in a PDF format.

5. Operational and Device Checks

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(f)	5.1 Are their operational system checks to enforce permitted sequencing of steps and events, if required?	N/A		N/A	It is the user's responsibility to designate and enforce procedural controls.
Part 11 11.10(g)	5.2 Are their 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?	S	Part 211, 68 b	Yes	The identity of the operator performing actions within the system is recorded in both the audit trail and activity log. Activities such as entering, modifying, and confirming data are tracked along with the operator's identity, date, and time. The Fragment Analyzer Controller Software 5.0.0 and ProSize Data Analysis Software 6.0.0 Security Module do not include content management. As a result, data deletion performed outside the system cannot be tracked. It is the user organization's responsibility to manage and control the deletion of data files.
Annex 11	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S.U	Annex 11, 12.4	Yes	The audit trail and activity log record all relevant entries in a chronological, human-readable, and easily understandable format. Users have the option to apply filters to find specific and meaningful activities.
Part 11 11.10(h)	5.4 Does the system allow use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction?	S	There are two equally valid interpretations of this requirement. Systems should be designed such that: 1. Proper communication is confirmed between the computer and the "source" of data input (i.e., the instrument) prior to transmission of instructions to or data from the "source." 2. Regulated records created by the system must unambiguously indicate the "source" of the data (i.e., which instrument or component generated the data.)	Yes	1. The system is designed to continually ensure a valid connection between the instrument and the computer workstation. 2. The system is designed to detect the connected Fragment Analyzer model and serial number and records this information in the activity log, measurement file, and audit trail as the data source.
Part 11 11.10(i)	5.5 Is their documented evidence that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	U	China GMP 18 Brazil 571	N/A	It is the user's responsibility to maintain documented evidence that the persons who develop, maintain, or use electronic record and electronic signature systems have the education, training, and experience needed to perform these tasks. Agilent software professionals involved in development of Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module have received training in relevant aspects of data integrity.

5. Operational and Device Checks continued

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.10(j)	5.6 Is there a written policy that holds individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification? 5.7 Have employees been trained on this procedure? (Implied requirement of Part 11 11.10(j))	U		N/A	It is the User's responsibility to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures. It is the user's responsibility to train their staff on this procedure.
Part 11 11.10(k)	5.7 Are their 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.	U	China GMP 161 第五章系统 第十七条计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评 估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。主要变更 应当经过验证。 第五章系统 第十一条应当有详细阐述系统的文件（必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序相接。	N/A	It is the user's responsibility to establish systems documentation controls. Agilent maintains development and testing documentation for Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module. The user organization is expected to maintain documentation of their system and associated changes in situ through proper change control procedure. If the user organization decides to upgrade the software version the system activity log will record the changes to the system with time sequenced entries.

6. Data Integrity, Date and Time Accuracy

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Annex 11	6.1 Do computerized systems that ex-change data electronically with other systems include appropriate built-in checks for the correct and secure entry and processing of data?	N/A	Annex 11.5	N/A	The system is designed to operate independently as standalone and does not exchange data with other systems.
Annex 11	6.2 Is there an additional check on the accuracy of the data? This check may be done by a second operator or by validated electronic means.	S.U	Annex 11-6 Brazil GMP 580 ICHQ7- 5.45 第五章系统 第十五条当人工输入关键数据时（例如在称重过程中输入物料的重量和批号），应当复核输入记录以确保其准确性。这个复核可 以由另外一个操作人员完成，或采用经验证 的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。	Yes	Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module allows for multi-user and multi-level-role-based review and approval using an eSignature workflow.
Part 11 11.10(e) 11.50(a)	6.3 Are controls established to ensure that the system's date and time are correct?	S.U	Annex 11.14	Yes	Agilent recommends that the system be configured to reference a timeserver to ensure accuracy of the system date and time. This is configured in and controlled by the operating system.
Part 11 11.10(e) 11.50(a)	6.4 Are timestamps with a clear understanding of the time zone reference used implemented for systems that span different time zones?	S	Annex 11.14	Yes	All time data is stored, in Coordinated Universal Time (UTC) and displayed with the local offset at the site of creation.

7. Control for Open Systems (Only Applicable for Open Systems)

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.30	7.1 Are their procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt?	U		N/A	Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module is not intended to be deployed as an "Open" system as per 21 CFR Part 11 11.3(b)(9)
Part 11 11.10(e) 11.50(a)	7.2 Are their 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?	U		N/A	Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module is not intended to be deployed as an "Open" system as per 21 CFR Part 11 11.3(b)(9)

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Annex 11	8.1 When electronic signatures are used, do they have the same impact as hand- written signatures within the boundaries of the company? Are they permanently linked to their respective record? Do they include the time and date that they were applied?	S.U	Annex 11.14 ICH Q7.6.18 第五章系统 第二十三条电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。	Yes	The user organization must establish the legal impact of electronic signatures. Signatures are permanently linked to their respective electronic records. Signed electronic records show the name of the signer, and date and time the signature was executed, and the meaning of the signature.
Part 11 11.50 (a)	8.2 Do signed electronic records 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 were executed? and 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	S		Yes	Signed electronic records show the name of the signer, and date and time the signature was executed, and the meaning of the signature. User organizations are allowed to generate reports of signed data files in a PDF and print format.
Part 11 11.50 (b)	8.3 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 are they included as part of any human readable form of the electronic record (such as electronic display or printout)?	S		Yes	Signed electronic records show the name of the signer, and date and time the signature was executed, and the meaning of the signature. User organizations are allowed to generate reports of signed data files in a PDF and print format.
Part 11 11.70	8.4 Are electronic signatures and handwritten signatures 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?	S.U		Yes	Linking handwritten signatures and electronic signatures is the user's organization responsibility. However electronic signatures once applied to the data file are permanently embedded in the result.
Part 11 Preamble	8.5 Is there a user-specific automatic inactivity disconnect measure that would "de-log" the user if no entries or actions were taken within a fixed short timeframe?	S	Part 11 Preamble section 124	Yes	Automatic session locking enables the user organization to configure a time after which the user is automatically locked out.

9. Electronic Signatures General Requirements and Signature Components and Controls

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	S		Yes	The system prevents duplicate user IDs, ensuring each user has a unique login and signature that cannot be used by another user. Users can be deactivated upon leaving the system/company.
Part 11 11.100(b)	9.2 Does the organization verify the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	U		N/A	It is the responsibility of the user organization to verify the identity of staff before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature.
Part 11 11.100 (c)	9.3 Are persons using electronic signatures, prior to or at the time of such use, certified 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? 9.4 Do persons using electronic signatures, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	U		N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.
Part 11 11.200(a) (1)	9.5 Do electronic signatures that are not based upon biometrics employ at least two distinct identification components such as an identification code and password?	S		Yes	Both identification (user ID) and password are required to make an electronic signature.
Part 11 11.200(a) (1) (i)	9.6 When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components?	S		Yes	Both identification (user ID and password) are required to make an electronic signature. However, the user ID is prefilled based on the log in credential for the users.
Part 11 11.200(a) (1) (i)	9.7 When an individual executes a series of signings during a single, continuous period of controlled system access, are subsequent signings executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?	S		Yes	Both identification (user ID and password) are required to make an electronic signature.
Part 11 11.200(a) (1) (ii)	9.8 When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	S		Yes	Both identification (user ID) and password) are required to make all electronic signatures.

9. Electronic Signatures General Requirements and Signature Components and Controls continued

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.200(a) (2)	9.9 Are controls in place to ensure that electronic signatures that are not based upon biometrics are used only by their genuine owners?	S.U		Yes	It is the user organization's responsibility to ensure that user names and passwords are known only by the assigned individuals and are traceable to individual users.
Part 11 11.200(a) (3)	9.10 Are the electronic signatures 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?	S		Yes	Misuse of electronic signatures by anyone other than the owner is only possible if the users credentials are obtained.
Part 11 11.200(b)	9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	N/A		N/A	Biometric authentication is not supported in Fragment Analyzer controller software 5.0.0 and ProSize Data analysis software 6.0.0 Security Module.

10. Controls for Identification Codes and Passwords

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Part 11 11.300(a)	10.1 Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	S		Yes	Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module does not allow duplicate user IDs.
Part 11 11.300(b)	10.2 Are controls in place to ensure that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	S		Yes	Password expiration is configurable using Active Directory integration. The user organization should configure password expiration based on a documented risk assessment.
Part 11 11.300(c)	10.3 Are their procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromise 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?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方 能进行操作。	N/A	It is the responsibility of the user organization to establish these procedures.
Part 11 11.300(d)	10.4 Are their transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts of their unauthorized use to the system security unit, and, as appropriate, to organizational management?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方 能进行操作。	N/A	It is the responsibility of the user organization to establish these transaction safeguards.
Part 11 11.300(e)	10.5 Are their controls for 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?	U		N/A	It is the responsibility of the user organization to establish controls to test devices initially as well as periodically to ensure they function properly and have not been altered in an unauthorized manner.

11. System Development and Support

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No/Partially	If yes, how, specifically, is the requirement satisfied using Fragment Analyzer Software Security Module? If no, what is the recommendation to customers?
Annex 11	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	S	Annex 11 4.5 Brazil GMP 577 GAMP 5 第二章原则 第四条企业应当注重计算机化系统供应商的管理，制定相应的操作规程。供应商提供产品或服务时（如安装、配 置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。	Yes	Fragment Analyzer controller software 5.0.0 and ProSize data analysis software 6.0.0 Security Module have been developed according to the ISO 9001 Quality Management Standard.
Brazil	11.2 Is there a formal agreement when the software supplier subcontracts software and maintenance services. Does the agreement include the contractor's responsibilities?	S	Brazil GMP 589 This is a shared responsibility between the system supplier and the user organization. The supplier must have such an agreement with the subcontractor, and the user must verify that the agreement is in place. 第二章原则 第四条企业应当注重计算机化系统供应商的管理，制定相应的操作规程。供应商提供产品或服务时（如安装、配 置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。	Yes	Agilent requires formal agreements with all suppliers. (Ref. section 8.4 and 8.5 of the Agilent Quality Manual).
ICH Q10	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	S	ICHQ10, 2.7 c *Note: If applicable to your product*	Yes	Agilent requires formal agreements with all suppliers (Ref. section 8.4 of the Agilent Quality Manual).
ICH Q10	11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined?	S	ICHQ10, 2.7 c *Note: If applicable to your product*	Yes	Agilent requires formal agreements with all suppliers (Ref. section 8.4 of the Agilent Quality Manual).
Part 11 11.10(i)	11.5 Are personnel developing and supporting software trained?	S	This is a shared responsibility between the system supplier and the user organization. The supplier must ensure its staff is trained, and the user should have assurance, e.g., through audits that SW developers are trained and that this training is documented. 第三章人员 第五条计算机化系统的“生命周期”中所涉及的各种活动，如验证、维护、管理等，需要各相关的职能部门人员之间的紧密合作。在职责中涉及使用和管理计算机化系统的人员，应当接受相应的使用和管理培训。确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训 和指导。	Yes	All Agilent personnel are required to be trained (Ref. section 7.2 and 8.2 of the Agilent Quality Manual).

References

1. R. A. Botha and J. H. P Eloff. Separation of duties for access control enforcement in workflow environments. IBM Systems Journal– End-to-end security. 40 (3), 666-682. (**2001**).
2. U.S. Food and Drug Administration. CFR - Code of Federal Regulations Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A— General. Part 11 Electronic Records; Electronics Signatures [Online] https://www.accessdata.fda. gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11.
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. The Rules Governing Medicinal Products in the European Union **EudraLex** Volume 4.
4. Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. [Online] https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/annex11_01-2011_ en.pdf.

For more information, please visit
www.agilent.com/genomics/fragment-analyzer-security-module

PR7001-3813

Published in the USA, February 04, 2025
5994-8118EN

Agilent
Trusted Answers