White Paper

Agilent
Trusted Answers

Support for Title 21 CFR Part 11 and Annex 11 Compliance: TapeStation Software Revision 5.1 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 organizations.

Released in 1997, 21 CFR Part 11 has been enforced since 1999. 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 the Agilent TapeStation system whose organizations must comply with these regulations. TapeStation software revision 5.1 Security Module controls acquisition and processing of TapeStation system data. It is the responsibility of the user and their organization to ensure that the functionalities provided by the TapeStation software revision 5.1 Security Module are used appropriately to achieve compliant operation for laboratory data acquisition and processing. In addition to the technical controls the TapeStation software revision 5.1 Security Module provides, the user organization must establish procedural controls – standard operating procedures (SOPs) – to address relevant non-technical requirements. 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 the TapeStation software revision 5.1 Security Module supports users and their organizations in achieving 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

Security can be interpreted as "the right people, having the right access, to the right information."[1] 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 must be segregated and defined such that certain users have certain types of access to certain sets of data while potentially having different access to other data sets.

Workstation

TapeStation software is installed and configured in a workstation. The workstation configuration allows direct control of an instrument from a standalone PC workstation (laptop) without requiring a server-based network resource. All data is stored locally in the file system.

Attribution of work

Attribution of work refers to documenting the "who, what, when, where, and why?"[1] 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 implemented. 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

"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]

Appendix 1. Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations while using TapeStation software revision 5.1 Security Module.

Appendix I Table: Notes

Column one

The table addresses 21 CFR Part 11 requirements in the order that they are presented in the US FDA reference document.[2] Related requirements such as those found in EU Annex 11 follow each section of Part 11.[3]

Column two

For completeness, column two lists all requirements of 21 CFR Part 11, and other related global requirements. "System" refers to the analytical system used to acquire and process data.

Most requirements are fulfilled by either technical controls (for example, software functionality) or procedural controls (for example, SOPs). Technical controls are controls provided by the software and hence the software supplier, while procedural controls are the responsibility of the user organization. 21 CFR Part 11 requirements listed in bold are requirements addressed by technical controls. Other global requirements are listed in regular font. Requirements that must be addressed by procedural controls are listed in blue.

Column three

Some requirements involve both technical and procedural controls. Responsibilities for each requirement are listed in column three. "S" refers to analytical system supplier. "U" refers to the user organization. Rows containing requirements that must be exclusively addressed by the user organization are shown in blue. Blue may also be technical controls the user will be responsible to implement.

Column four

If available and where appropriate, related global requirements and comments are provided in column four.

Column five

Column five indicates with a "yes" or "no" whether the requirement can be satisfied using the technical controls provided in TapeStation software revision 5.1 Security Module. N/A is not applicable to the TapeStation software revision 5.1 Security Module.

Column six

Column six explains how the regulatory requirement can be satisfied using the technical controls provided by TapeStation software revision 5.1 Security Module. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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. For example, validation activities during development and related documentation.	Partially Yes	Agilent Technologies has extensively verified the performance of the TapeStation software revision 5.1 Security Module using tests that evaluate accuracy, reliability, and consistent performance. However, the user organization is required to validate their analytical system according to regulatory expectations. Agilent additionally offers IQ/OQ services. With respect to TapeStation software revision 5.1 Security Module, "regulated records" are: – Analysis parameters – Acquired data – Analysis results – Report templates – Associated audit trails/electronic signature – User management The product does not come with content management. It is the user organization's responsibility to maintain accuracy, reliability, and the ability to discern invalid or altered records.
Annex 11	1.2 Is infrastructure qualified?		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	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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.		Yes	Records are available printed on paper or electronically as a PDF file. However, the accuracy of the records post acquisition is the user organization's responsibility.
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	Yes	Records are available printed on paper or electronically as a PDF file.
Brazil	2.3 Are there controls to make sure that the data backup, retrieval, and maintenance process is duly carried out?	U.	Brazil 585.2	No	Backing up data is the user organization's responsibility.
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 user organization's responsibility to maintain the physical security of the raw data, meta data, and result data generated by the TapeStation 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.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability, and integrity?	U.	Annex 11.17	N/A	It is the responsibility of the user's organization to ensure data are checked during archival for accessibility, readability, and integrity.
Annex 11	2.6 If relevant changes are made to the system (for example, computer equipment or programs), is then the ability to retrieve the data ensured and tested?	S.U.	Annex 11.17	Yes	The system is designed to read data from legacy TapeStation software versions by import. The data of older versions before revision 5.1 does not contain an audit trail. It is user organization'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?	U.	Annex 11.7 .I Brazil GMP 584	N/A	It is user organization's responsibility to provide a secured data storage location.
Clinical guide	2.8 Are there controls implemented that allow for the reconstruction of the electronic source/raw documentation for FDA's review of the (clinical) study and laboratory test results?	N/A	Clinical Computer Guide F2 FDA Q&As	N/A	N/A

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

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Clinical guide	2.9 Does the information provided to the FDA fully describe and explain how source/raw data were obtained and managed, and how electronic records were used to capture data?	U.	Clinical Computer Guide F2 FDA Q&As	N/A	It is the responsibility of the user organization to describe how source/raw data were obtained and managed, and how electronic records were used to capture data.
Annex 11	2.10 Does the system allow for regular backups of all relevant data?	U.	Annex 11.7 .I China GMP 163 Brazil GMP 585 Part 211, 68 b	N/A	Backing up data is the responsibility of the user organization.
Annex 11	2.11 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	N/A	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.
Clinical Computer Guide	2.12 Are procedures and controls in place to prevent the altering, browsing, querying, or reporting of data by external software applications that do not enter through the protective system software?	S.U.	Clinical Computer Guide E	Yes	The system is designed to be a standalone system and does not exchange data with other systems.
Clinical Computer Guide	2.13 Are there controls implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software?	U.	Clinical Computer Guide F	N/A	Agilent has tested the TapeStation software in conjunction with Microsoft Defender. However, it is the responsibility of the user organization to implement anti-virus software.

3. Authorized Access to Systems, Functions, and Data

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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. Duplication of the user ID is detected and prevented by the system. Entry of both is required to access the system. However, it is the user organization's responsibility to clearly define roles and responsibilities to prevent conflict of interest.
	3.2 Is each user clearly identified, for example, through his/her own user ID and password?	S. U.	Several Warning Letters	Yes	Each user is identified by a unique ID and password combination. Duplication of the user ID is detected and prevented by the system. Entry of both is required to access the system. However, it is the user organization's responsibility to clearly define roles and responsibilities to prevent conflict of interest.
Clinical	3.3 Are there controls to maintain a cumulative record that indicates, at any point in time, the names of authorized personnel, their titles, and a description of their access privileges?	S.	Clinical Computer Guide 4	Yes	TapeStation software revision 5.1 Security Module can authenticate users through either the Windows Domain or locally in the application itself. Access privileges are set in the application and any changes are recorded in the activity log. Reports are available that show users' individual privileges and access rights. These reports can be useful for organizations required to perform periodic security reviews.

4. Electronic Audit Trail

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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	Yes	Creation and modification are recorded in a secure, computer-generated, time-stamped audit trail and activity log. Audit trails and activity log entries are created for all result data, system related changes, and changes to the report templates. However, renaming and deleting of data files is the user organization's responsibility to control and manage.
FDA GLP	4.2 Does the audit trail record who has made which changes, when, and why?	S.	FDA 21 CFF 58.130 e Clinical Computer Guide 2 Clinical Source Data 3	Yes	The audit trail includes the user ID, date, and time of the change, and before and after values with the reason for change. The activity log will record when and by whom the changes were made.
Annex 11	4.3 Can the system generate printouts indicating if any of the eRecords have been changed since the original entry?	S.	Annex 11, 8.2	Yes	TapeStation software revision 5.1 Security Module records all the changes made to system and data files in activity log and audit trails. The system allows users to export and print.
FDA GMP	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.	Part 211.194 8b	Yes	Changes must be made directly to the data file. Method templates are not supported in revision 5.1. However, every change to the data file requires an eSignature and a reason for change. Both are captured in the audit trail along with the reason for change.
	4.6 Is the audit trail function configured to always be on and can it not be switched off by system users?	S.	Warning Letter	Yes	Once audit trails are activated during the installation, they cannot be turned off by the system users.
Annex 11	4.7 Is audit trail available in a generally intelligible form for regular review?	S.	Annex 11, 9	Yes	The system activity log and audit trail record all the relevant entries in a chronological and human readable format. Users can choose to filter to look for relevant and meaningful activities.
	4.8 Can audit trail contents be configured such that only relevant activities are recorded for realistic and meaningful review of audit trail information?	S.	Implicitly required by Annex 11 with many warning letters related to review of audit trail.	Yes	The system activity log and audit trail record all the relevant entries in a chronological and human readable format. Users can choose to filter to look for relevant and meaningful activities.
Part 11 11.10(e)	**4.9 Is previously recorded information left unchanged when records are changed?**	S.		Yes	All changes made to the system and electronic records are recorded in an audit trail and system activity log, and these entries cannot be changed once recorded.
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 the user organization's responsibility to maintain throughout their retention period, and is readily available to view and analyze.
Part 11 11.10(e)	4.11 Are audit trails available for review and copying by the FDA?	S.		Yes	Audit trails can be reviewed and printed in a PDF format.
Annex 11	4.12 Is it possible to obtain clear printed copies of electronically stored eRecords (for example, eAudit trail)?	S.	Annex 11, 8.1	Yes	Audit trails can be reviewed and printed in a PDF format.

5. Operational and Device Checks

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Part 11 11.10(f)	5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required?	N/A		N/A	It is the user organization's responsibility to designate and enforce procedural controls.
Part 11 11.10(g)	**5.2 Are there 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 system supports configurable user roles that control system access at a detailed level. Access and privileges can be segregated and defined by the user organization, however segregations of roles and responsibility is the user organization's responsibility.
	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	Activities pertaining to entering, changing, archiving, and confirming data are tracked through the identity of the operator with dates and times recorded in audit trail and activity logs. The TapeStation Security Module revision 5.1 does not come with content management. It is the user organization's responsibility to control deletion of data files.
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 (for example, 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 (for example, 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 identify which TapeStation model and serial number is connected to the computer workstation and indicates this in the activity log, measurement file, and audit trail of the data source.
Part 11 11.10(i)	5.5 Is there documented evidence that individuals 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 organization's responsibility to maintain documented evidence that the individuals 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 TapeStation software revision 5.1 Security Module have received training in relevant aspects of data integrity.
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, to determine record and signature falsification?	U.		N/A	It is the user organization's responsibility to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
	5.7 Have employees been trained on this procedure?	U.	Implied requirement of Part 11 11.10(j)	N/A	Is it the user organization's responsibility to train their staff on this procedure.
Part 11 11.10(k)	5.8 Are there appropriate controls for system 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 documenting time-sequenced development and modification of system documentation.	U.	China GMP 161	N/A	It is the user organization's responsibility to establish system documentation controls.

5. Operational and Device Checks *continued*

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Part 11 11.10(i)	**5.9 Are there revision and change control procedures to maintain an audit trail documenting time-sequenced development and modification of system documentation?**	S.U.		Yes	Agilent maintains development and testing documentation for the TapeStation software revision 5.1 Security Module. The user organization is expected to maintain documentation of their system and associated changes in situ through proper change control procedures. 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	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Annex 11	6.1 Do computerized systems that exchange 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 be a standalone system 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	Yes	TapeStation software revision 5.1 Security Module allows for multi-user and multi-level, role-based review and approval using an eSignature workflow.
Clinical Computer Guide	6.3 Are controls established to ensure that the system's date and time are correct?	U.	Clinical Computer Guide D.3	N/A	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.
Clinical Computer Guide	6.4 Can date or time only be changed by authorized personnel, and is such personnel notified if a system date or time discrepancy is detected?	U.	Clinical Computer Guide D.3	N/A	TapeStation software revision 5.1 Security Module uses the time of the underlying Windows operating system. It is the user organization's responsibility to: – Limit access controls of Windows time settings to only authorized personnel – Maintain procedural controls for setting and maintaining the accuracy of Windows time
Clinical Computer Guide I	6.5 Are timestamps with a clear understanding of the chosen time zone reference implemented for systems that span different time zones?	S.	Clinical Computer Guide D.3	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	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Part 11 11.30	7.1 Are there 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	TapeStation software revision 5.1 Security Module is not intended to be deployed as an "open" system per 21 CFR Part 11.3(b)(9).
Part 11 11.30	7.2 Are there 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	TapeStation software revision 5.1 Security Module is not intended to be deployed as "open" system as per 21 CFR Part 11.3(b)(9).

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

Part 11 and Others	Requirement	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
Annex 11	8.1 When electronic signatures are used, do they have the same impact as handwritten 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 07 .6.18	Yes	The user organization must establish the legal impact of electronic signatures. Signatures are permanently linked to their respective records. Signed electronic records show the name of the signer, the 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 signature that clearly indicate all of the following: (1) The printed name of the signer? (2) The date and time the signature was 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, the 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 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, the date and time the signature was executed, and the meaning of the signature. User organizations are able to generate reports of signed data files in a PDF and print format.
Part 11 11.70	8.4 Are electronic and handwritten signatures linked to their respective electronic records to ensure that they cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	S.U.		Yes	Linking handwritten and electronic signatures is the user organization's responsibility. However, electronic signatures, once applied to the data file, are permanently embedded in the result and reports.
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	Supplier (S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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	Each user has a unique login and password. Thus a unique signature that cannot be used by another user. Users can be deactivated once they leave the system.
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 individuals using electronic signatures, prior to or at the time of such use, certified by the agency that the electronic signatures in their system, used on or after 20 August 1997, are intended to be the legally binding equivalent of traditional handwritten signatures? 9.4 Do individuals 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 components (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 components (user ID and password) are required to make all electronic signatures. However, the user ID is prefilled based on the login 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 components (user ID and password) are required to make all electronic signatures. However, the user ID is prefilled based on the log in credential for the users.
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 electronic signature components?**	S.		Yes	Both identification components (user ID and password) are required to make all electronic signatures. However, the user ID is prefilled based on the log in credential for the users.
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.		Yes	Both identification components (user ID and password) are required to make all electronic signatures.
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 TapeStation software revision 5.1 Security Module.

10. Controls for Identification Codes and Passwords

Part 11 and Others	Requirement	Supplier(S) or User organization (U) responsibility	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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	TapeStation software revision 5.1 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 (for example, to cover such events as password aging)?	U.		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 there procedures to electronically de-authorize 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?	U.		N/A	It is the responsibility of the user organization to establish these procedures.
Part 11 11.300(d)	10.4 Are there 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.		N/A	It is the responsibility of the user organization to establish these transaction safeguards.
Part 11 11.300(e)	11.5 Are there 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	Supplier(S) or User organization (U) responsibility	Other associated regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied using TapeStation software 5.1 Security Module? If no, what is the recommendation?
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 This is a shared responsibility between the system supplier and the user organization. The user should require the supplier to provide documented evidence that software is developed within the framework of a quality management system (QMS).	Yes	TapeStation software revision 5.1 Security Module has been developed according to the ISO 9001 Quality Management Standard (Ref. section 1.1 of the Agilent Quality Manual).
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.	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	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	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?		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, for example, through audits that software developers are trained and that this training is documented.	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; J. H. P Eloff. Separation of duties for access control enforcement in workflow environments. IBM Systems Journal - End-to-end security. **2001.** 40 (3), 666-682.
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. https:// gov/scripts/ cdrh/cfdocs/ cfcfr/ CFRSearch .cfm?CFRPart=l 1 (accessed Nov 04, 2015).
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. Eudralex. The Rules Governing Medicinal Products in the European Union. Volume 4. Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. http://ec .europa.eu/health/ files/ eudralex/vol-4/annexl 7-01-201L en.pdf (accessed Nov 04, 2015).

www.agilent.com/genomics/tapestation

For Research Use Only. Not for use in diagnostic procedures.
PR7001-0349

Document Number: D0028138
Revision: A.00

Published in the USA, February 01, 2023
5994-5705EN

Agilent
Trusted Answers