White Paper

Agilent
Trusted Answers

Support for Title 21 CFR Part 11 and Annex 11 compliance: Agilent MassHunter for LC/MS

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 Agilent MassHunter for LC/MS systems whose organizations must comply with these regulations. MassHunter for LC/MS controls acquisition and processing of triple quadrupole LC/MS systems. It is the responsibility of the user and their organization to ensure that the functionalities provided by MassHunter for LC/MS are used appropriately to achieve compliance-readiness for laboratory data acquisition and processing. In addition to the MassHunter technical controls, the user organization must establish procedural controls--standard operating procedures (SOPs)--to address relevant non-technical requirements. Governance, for example as an internal audit program, must also be established to assure that system operators follow the SOPs.

Appendix 1 provides a detailed description of how MassHunter for LC/MS 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 refers to 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 must be able to be segregated and defined such that certain users have certain types of access to certain sets of data while having different access to other data sets.

"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]

For example, in MassHunter LC/MS Acquisition, it is possible to restrict a user from editing a method, but the same user can create and edit a sequence. In OpenLab ECM, it is possible to restrict a user to only specific information within a specific OpenLab ECM Location and the file access within that location.

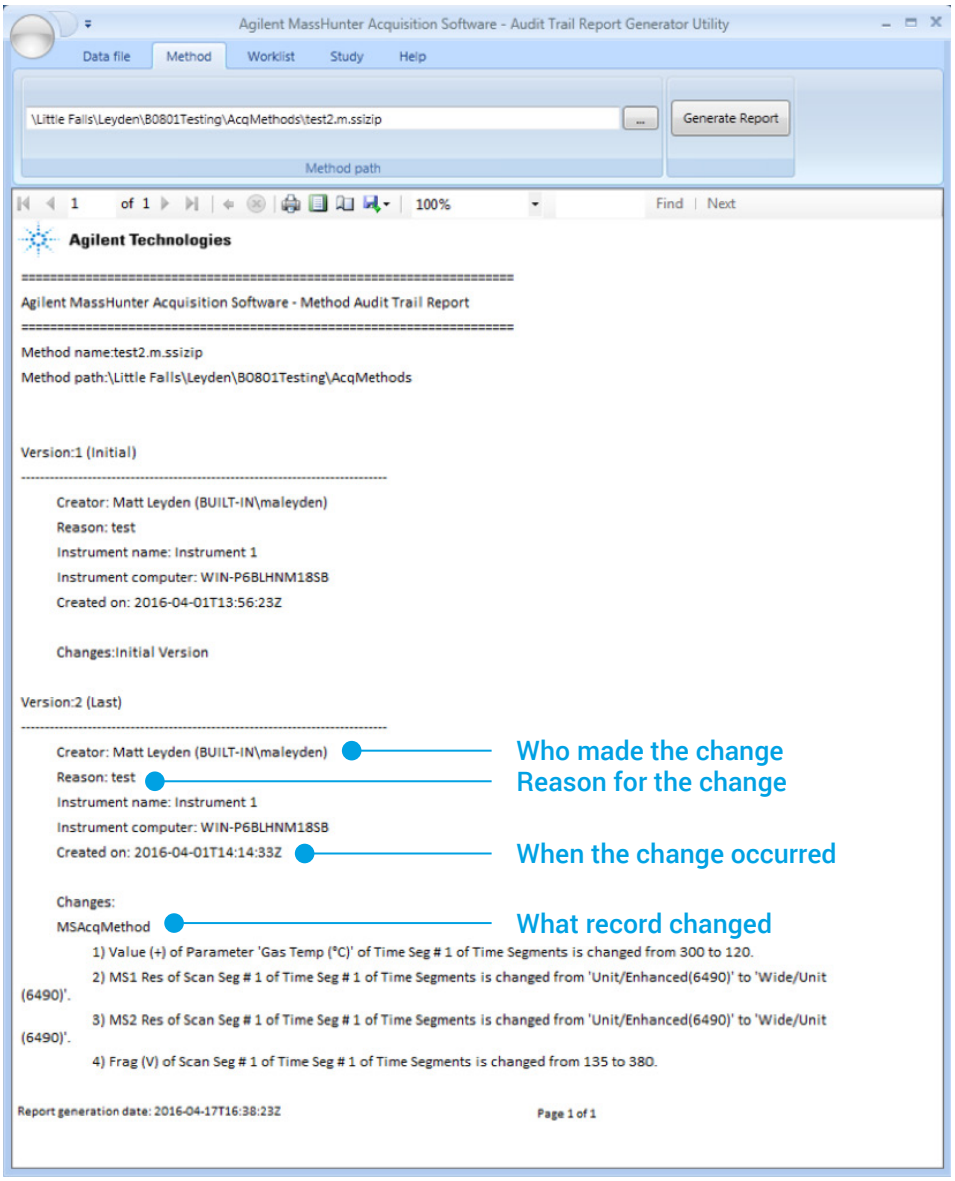
Attribution of work

Attribution of work refers to documenting the "Who, what, when, where and why?" of work performed. This is usually done via the use of automated audit trail functionality. Automated audit trails independently record user's 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.

An example of the Who, What, When, Where, and (optionally) Why can be seen in the MassHunter LC/MS Acquisition example. In this example, the Administrator did not require a reason for the change of the acquisition method.

[1] *For the context of this whitepaper, MassHunter for LC/MS consists of MassHunter LC/MS Acquisition, and MassHunter Quantitative Analysis installed with the "compliance" toolset and connected with OpenLab ECM. The technical controls discussed in this whitepaper apply to specific versions of each module as documented in MassHunter.*



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 the signature (such as review, approval, responsibility, or authorship).
- Are present whenever the signed records are displayed or printed

Without eSignatures, a lab is committing to a hybrid paper/electronic record solution.

The following outlines the minimum software requirements for LC/TQ compliance mode. The latest shipping software is recommended to enable enhancements and defect fixes. At a minimum, MassHunter LC/MS Acquisition B.08.01, Quantitative Analysis B.08, and OpenLab ECM 3.4.1 SP2 HotFix 3 are required for LC/TQ compliance mode. To use OpenLab ECM 3.5.5 with LC/TQ, a minimum of MassHunter LC/MS Acquisition 10 and Quantitative Analysis 10 is required. Ultivo compliance mode will require at least MassHunter LC/MS Acquisition 1.1, Quantitative Analysis 10, and OpenLab ECM 3.5.5. Please consult your sales representative for a compatibility assessment of your current software.

Appendix 1. Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations using MassHunter for LC/MS.

Appendix 1 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]

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 (i.e. software functionality) or procedural controls (i.e. 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 requirements listed in bold are requirements addressed by technical controls. Other global requirements are listed in regular font.

Column three

Responsibilities for each requirement are listed in column three. "S" refers to analytical system vendor. "U" refers to the user organization. Use of "S" and "U" implies a combination of both technical and procedural controls.

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 MassHunter for LC/MS. Not applicable (N/A) is used when a requirement must be addressed by procedural controls.

Column six

Column six explains how the regulatory requirement can be satisfied using the technical controls provided by MassHunter for LC/MS. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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 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。	Yes	While Agilent software is accompanied by a Declaration of Software Validation, stating that the software "… was developed and tested according to the Agilent Technologies Lifecycle. Lifecycle checkpoint deliverables were reviewed and approved by management. The product was found to meet its functional and performance specifications, and release criteria at release to shipment." this statement in no way releases the customer from their regulatory responsibility to validate computerized systems for their intended use. Agilent has a range of compliance and validation services available for purchase, see **www.agilent.com/chem/services** for more details.

[2] *The "**…ability to discern invalid or altered records**." section of this regulation is discussed separately for clarity.*

1. Validation *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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		Yes	The integrated solution of MassHunter with OpenLab ECM incorporates the use of byte- order dependent check sums at each file transfer operation to ensure that record transfers are valid between the components. MassHunter Software includes the ability to check the integrity of files in a batch. The following MassHunter records contain checksum information that can be used to determine if the contents of the associated record component have been altered. Acquisition Methods Acquired Data Acquisition Worklists Acquisition Studies Analysis Methods Analysis Results
Annex 11	1.2 Is infrastructure qualified?	U	Annex 11.Principle B Brazil GMP 577	N/A	Qualification of infrastructure such as servers and networks are the responsibility of the user organization.

2. Accurate Copies and Secure Retention and Retrieval of Records

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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	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	The system generates the following records that can be viewed (V) and printed (P); Tune Parameters (V and P) Acquisition Methods (V and P) Acquired data (V and P) Analysis Results (V and P) Analysis Reports (V and P) Worklist (V and P) Study (V and P) Instrument logs (V and P) Audit Trails (V and P) Electronic signatures (V (all) and P (PDF only*)) *Print is only available for signatures embedded into Adobe's signature into PDF add on. In addition to the binary raw data, MassHunter stores additional information (metadata) regarding the state of the system at the time of analysis with each data file.
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	MassHunter Acquisition for LC/MS TQ, MassHunter Quantitative Analysis, and OpenLab ECM can generate printed copies of all electronically stored e-records.
Brazil	2.3 Are there controls to make sure that the data backup, retrieving and maintenance process is duly carried out?	S, 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。	N/A	It is the responsibility of the user organization to control data backup, retrieving and maintenance.

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

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
Part 11 11.10(c)	**2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?**	S, U	China GMP 163	Yes	Records (methods, worklists, studies, raw data, metadata, and result data) generated by MassHunter are stored and managed in OpenLab ECM. MassHunter stores all raw data, metadata, and result data automatically in OpenLab ECM immediately after acquisition, and after each interactive review or automated reprocessing. Data stored in OpenLab ECM resides in a managed, secure storage location. All file actions, including file deletion, are tracked through the OpenLab ECM audit trail. All records are protected in the OpenLab ECM environment and are retrieved from the OpenLab ECM server on review. It's the user organization's responsibility to manage the physical security and controlled access to OpenLab ECM.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability and integrity?	U	Annex 11.17	N/A	It's the user organization's responsibility to check data during archival for accessibility, readability, and integrity.
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	N/A	Agilent's Software Development Lifecycle includes upgrade testing that ensure complete data retrieval in Agilent's test environment. It is the user organization's responsibility to test and ensure data retrieval is intact after server upgrades in their environment.
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。	N/A	It is the user organization's responsibility to prevent physical damage to hardware that generates and retains data. It is also the user organization's responsibility to implement backup and disaster recovery mechanisms. Electronically, data is secured by controlled access via authentication and authorization. Secured communication protocols are used to protect data transfer between system components. OpenLab ECM has a mechanism to notify admin after a set number of failed login attempts.
Annex 11	2.10 Does the system allow performing regular back-ups of all relevant data?	S	Annex 11.7.1 China GMP 163 Brazil GMP 585 Part 211, 68 b	Yes	OpenLab ECM has facilities to allow for the administrator to perform periodic backups of the database.
Annex 11	2.11 Is the integrity and accuracy of backup data and the ability to restore the data checked during validation 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 the backed-up data, and also to check, validate and monitor restored data periodically.

3. Authorized Access to Systems, Functions, and Data

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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	MassHunter Acquisition for LC/MS TQ, MassHunter Quantitative Analysis, and OpenLab ECM have user-based access controls requiring a unique user name and password combination. It is the user organization's responsibility to configure and manage these users. MassHunter LC/MS Study Manager also allows submission of separate studies by different users during operation with the appropriate attribution of work.
	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	S, U	Several Warning Letters	Yes	MassHunter and OpenLab ECM authentication is linked to the Microsoft Windows® user management (user name and password) or OpenLab ECM User Management (user name and password)– the authorized user is part of the record. The system uniquely identifies each user with the user ID and password. It is the user organization's responsibility to ensure unique identities of authorized persons.

4. Electronic Audit Trail

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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	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	MassHunter has a secure, computer-generated, time-stamped audit trail for the following records: LC/MS Acquisition Method: Yes LC/MS Acquisition Worklist: Yes LC/MS Acquisition Raw Data: Yes LC/MS Acquisition Study: Yes LC/MS Acquisition Configuration: Yes MassHunter Quant Results: Yes MassHunter Quant Method: Yes OpenLab ECM eSignature: Yes File actions performed via OpenLab ECM, including file deletion, are tracked through the OpenLab ECM audit trail.
FDA GLP	4.2 Does the audit trail record who has made which changes, when and why?	S	FDA 21 CFF 58.130 e	Yes	The system can be configured so that the user is required to enter a reason for changes to the records below. The reason can be either freeform or predefined by the system administrator. LC/MS Acquisition Method: Yes LC/MS Acquisition Worklist: Yes LC/MS Acquisition Study: Yes LC/MS Acquisition Configuration: Yes MassHunter Quant Batch: Yes, including any changes to the embedded method. MassHunter Quant Method: Yes

4. Electronic Audit Trail *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
Annex 11	**4.3 Can the system generate printouts indicating if any of the e-records has been changed since the original entry?**	S	Annex 11, 8.2	Yes	MassHunter Acquisition for LC/MS TQ, MassHunter Quantitative Analysis, and OpenLab ECM each have this capability.
FDA GMP	4.4 Does the audit trail include any modifications of an established method employed in testing?	S	Part 211.194 8b	Yes	MassHunter Acquisition for LC/MS TQ, MassHunter Quantitative Analysis, and OpenLab ECM each have this capability.
FDA GMP	4.5 Do such records include the reason for the modification?	S		Yes	The system can be configured so that the user is required to enter a reason for changes to the records below. The reason can be either freeform or predefined by the system administrator. LC/MS Acquisition Method: Yes LC/MS Acquisition Worklist: Yes LC/MS Acquisition Study: Yes LC/MS Acquisition Configuration: Yes MassHunter Quant Batch: Yes, including any changes to the embedded method. MassHunter Quant Method: Yes
	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	Yes	MassHunter LC/MS Acquisition and MassHunter Quantitative Analysis audit trails are always on when using the regulated workflow. Changing this requires reinstallation of the software with different options.
Annex 11	4.7 Is audit trail available to a generally intelligible form for regular review?	S	Annex 11, 9	Yes	All audit trails are human readable.
	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 and many warning letters related to review of audit trail.	Yes	Audit trail contents are preprogrammed and not configurable. Audit trails are linked to the record – only audit trail entries relevant to the record are viewable.
Part 11 11.10(e)	**4.9 Is previously recorded information left unchanged when records are changed?**	S		Yes	Records are saved to OpenLab ECM. Revisions are created when edits are made, and data is never over-written. OpenLab ECM maintains history of all versions of the record. MassHunter audit trails capture old value and new value when records are changed.
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	MassHunter audit trails are linked with the record and are preserved so long as the record is kept in OpenLab ECM. OpenLab ECM allows for configurable retention policies to meet data lifecycle management.
Part 11 11.10(e)	**4.11 Is audit trail available for review and copying by the FDA?**	S		Yes	MassHunter audit trails can be reviewed and printed. Refer to the administrator guide for details.
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 examined by any authorized party.

5. Operational and Device Checks

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation to customers?
Part 11 11.10(f)	**5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required?**	S		Yes	The system supports standard MassHunter workflows where a series of steps need to be followed. Only users with specific permissions are entitled to run the system. It is possible for the lab to enforce common workflow restrictions by User Group. MassHunter Acquisition and Quant operate based on methods, which can be restricted to prevent editing while permitting execution by users.
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	MassHunter and OpenLab ECM manage access and capabilities through permissions linked to the User login. Certain tasks, such as electronically signing a record or deletion of a file, require additional authority checks to perform the action. Users cannot gain access to the software modules of LC/MS MassHunter / OpenLab ECM without a valid user ID, password and account. Once logged in, that user's access to files and software functionality (including but not limited to signing a file, inputting values, or altering a record) is determined by the privileges assigned to the user.
	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S	Annex 11, 12.4	Yes	Operating system date and time are tracked through operating system logs.
Part 11 11.10(h)	**5.4 Does the system allow to use 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	The instrument identification, through serial number, instrument ID, and IP address, is recorded with the data and may be included in reports as required. 1. The system is designed to continually ensure a valid connection between the instrument and the computer workstation. 2. Identification of instrument components such as LC modules and MS instruments are supported in the system
Part 11 11.10(i)	**5.5 Is there 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, S	China GMP 18 Brazil 571	Yes	It is the responsibility of the user organization 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 personnel who develop MassHunter and OpenLab ECM are made aware of regulatory requirements as appropriate to their function.

5. Operational and Device Checks *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation to customers?
Part 11 11.10(j)	5.6 Is there a written policy that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification?	U		N/A	It is the responsibility of the user organization 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	It is the responsibility of the user organization to train their staff.
Part 11 11.10(k)	5.8 Are there appropriate controls over systems documentation including:(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	U	China GMP 161 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 responsibility of the user organization to establish systems documentation.
Part 11 11.10(i)	5.9 Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation?	S, U	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。	Yes	It's the user organization responsibility to document the validation and configuration efforts through version control documents (specification, protocol, traceability matrix, summary reports, etc.) Agilent follows the Agilent Product Lifecycle with defined documentation, programming and testing guidelines. Source Code and product lifecycle documents, with revision history, are maintained with commercial electronic document control systems for all releases.

6. Data Integrity, Date and Time Accuracy

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
There are no specific paragraphs in Part 11 that relate to this topic. This may apply to other regulatory requirements that are not addressed in this document.					
Annex 11	6.1 Do computerized systems exchanging data electronically with other systems include appropriate built-in checks for the correct and secure entry and processing of data?	S	Annex 11.5	Yes	The integrated solution of MassHunter with OpenLab ECM incorporates the use of byte- order dependent check sums at each file transfer operation to ensure that record transfers are valid between the components.
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	The integrated solution of MassHunter with OpenLab ECM incorporates the use of byte- order dependent check sums at each file transfer operation to ensure that record transfers are valid between the components.

7. Control for Open Systems (Only applicable for open systems)

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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?	S,U		N/A	MassHunter is not intended to be deployed as an open system as 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?	S		N/A	MassHunter is not intended to be deployed as an open system as per 21 CFR Part 11.3(b)(9).

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

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
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	eSignatures are applied in the OpenLab ECM client. Signatures are permanently linked to their respective records. They include time and date that they were applied. It is customer responsibility to define the meaning of an electronic 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 was executed? and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature?**	S		Yes	OpenLab ECM electronic signature manifestation includes: – The user ID in addition to the full name of the signer – The signer's title – The date and time that the signature was applied – The location where the signing occurred – The meaning of the signature
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 (*)	Electronic signatures in OpenLab ECM (Native and PDF‡) can be displayed. * Electronic Signatures in PDF are available for printing. ‡ Via eSignature Plug-in for Adobe Acrobat.

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
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		Yes	Signed records have a unique checksum that prevents signatures from being excised, copied or otherwise transferred. OpenLab ECM will not recognize a signature that was applied outside its own electronic signature plug-ins. The optional eSignature Plug-in for Adobe Acrobat encrypts the signature within the document to prevent the signature from being excised or copied to another document.
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	MassHunter LC/TQ Acquisition supports automatic lock-out of a user session after a period of inactivity. The time-out criteria may be configured by the administrator. This feature is available for LC/TQ Acquisition versions 10 and above, and Ultivo Acquisition versions 1.1 and above. MassHunter Quantitative Analysis supports automatic lock-out of a user session after a period of inactivity. The time-out criteria may be configured by the administrator. This feature is available for Quant versions B.09 and above. When in the locked state, automated operations within MassHunter LC/MS Acquisition, such as running a worklist, will continue with appropriate attribution of work. A user must authenticate to retain active control of the system.

9. Electronic Signatures General Requirements and Signature Components and Controls

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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, U		Yes	User names in OpenLab ECM are required to be unique and cannot be reused or reassigned to another individual. Whether OpenLab ECM uses the company's Windows® logins to validate users or OpenLab ECM administrated users, no two users can have the same user ID / password combination. It is the user organization's responsibility to govern the user name and password policy.
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	This is the user organization's responsibility.

9. Electronic Signatures General Requirements and Signature Components and Controls *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation to customers?
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	This is the user organization's responsibility.
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, U		Yes	Electronic Signature authentication within OpenLab ECM requires both a username and password.
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	When an individual within OpenLab ECM signs the first of a series of documents during a single period of controlled access the user is required to enter three signature components: user ID, password and meaning of signature.
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	When OpenLab ECM user executes a series of continuous electronic signatures, which are defined as signatures executed within a period of time determined by the system administrator, they are required to enter user ID, password and reason on the first signature only. Each subsequent signature requires only the user's password, which is known only to the user.
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	When OpenLab ECM user executes a series of non-continuous electronic signatures, which are defined as signatures executed outside of a period of time determined by the system administrator, they are required to enter user ID, password and meaning of signature on each signature.
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	OpenLab ECM and Windows can be configured such that an administrator can assign an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way the user ID / password combination is known only to the individual. Whether OpenLab ECM uses the company's Windows NT logins to validate users or OpenLab ECM administrated users, no two users can have the same user ID / password combination. It is the user's responsibility not to share usernames and passwords with other lab members.

9. Electronic Signatures General Requirements and Signature Components and Controls *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation to customers?
Part 11 11.200(a) (3)	**9.10 Are the electronic signatures 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?**	S, U		Yes	Yes. OpenLab ECM uses the user's user ID and password to initiate the electronic signature. An OpenLab ECM user's password is stored encrypted within the database and is displayed as asterisks in all locations within the software. OpenLab ECM can be configured such that an administrator can assign an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way the user ID / password combination is known only to the individual.
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?**	S		N/A	MassHunter and OpenLab ECM do not employ biometrics for user authentication.

10. Controls for Identification Codes and Passwords

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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, U		Yes	The MassHunter authentication is tied to Windows® User management, including use of domain level Users. If using Windows® user and group management, the administrator can configure Windows® password policy setup appropriately. Whether OpenLab ECM uses the company's Windows® domain logins to validate users or OpenLab ECM administrated users, no two users can have the same user ID / password combination.
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, U		Yes	MassHunter authentication uses Windows® domain authentication, as such password renewal interval is configured as part of the Windows® password policy setup. The administrator can define a time frame in which passwords are periodically revised automatically. Users are prevented from reusing passwords. Users administrated in OpenLab ECM can be configured such that passwords are automatically, periodically revised.
Part 11 11.300(c)	10.3 Are there procedures to electronically deauthorize 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	This is the user organization's responsibility.

10. Controls for Identification Codes and Passwords *(continued)*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or If no, what is the recommendation?
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 at 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	MassHunter authentication can use Windows® domain authentication, as such transaction safeguards can be configured as part of the Windows® password policy setup. It is the user organization's responsibility to configure the transaction safeguards for the Windows® system.
Part 11 11.300(e)	**10.5 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	N/A

11. System Development and Support

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied? or 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, U	Annex 11 4.5 Brazil GMP 577 GAMP 第二章原则 企业应当能够提供与供应商质量体系和审计信息相关的文件。	Yes	Agilent software is developed and tested according to the Agilent Technologies Lifecycle compliant to ISO 9001. Lifecycle checkpoint deliverables were reviewed and approved by management. The product was found to meet its functional and performance specifications, and release criteria at release to shipment.
Brazil	11.2 Is there a formal agreement in case of the software supplier subcontracts software and maintenance services. Does the agreement include the contractor's responsibilities?	S, U	Brazil GMP 589 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 for all suppliers and follows ISO 9001 supplier quality management policy.
ICH Q10	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	S, U	ICHQ10, 2.7 c	Yes	Agilent requires formal agreements for all suppliers and follows ISO 9001 supplier quality management policy.
ICH Q10	11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined?	S, U	ICHQ10, 2.7 c	Yes	Agilent requires formal agreements for all suppliers and follows ISO 9001 supplier quality management policy.
Part 11 11.10(i)	11.5 Is personnel developing and supporting software trained?	S, U	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	Yes – all field engineers involved with installing the MassHunter product must be trained on the G3339AA MassHunter Access Control product.

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 (accessed November 19, 2018).

www.agilent.com/chem/masshunter

Printed in the USA, January 17, 2019
5994-0573EN

Agilent

Trusted Answers