White Paper

Agilent
Trusted Answers

Support for Title 21 CFR Part 11 and Annex 11 Compliance: Agilent MassHunter for LC/TQ, LC/TOF, and LC/Q-TOF Systems

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 Networked Workstation for Tandem Quadrupole, TOF, and Q-TOF LC/MS systems revision 11.0 or higher whose organizations must comply with these regulations. MassHunter Networked Workstation consists of:

- MassHunter Acquisition for TOF and Q-TOF LC/MS systems 11.0 or higher controls and acquires data from Agilent's Time of Flight (TOF) or Quadrupole Time of Flight (Q-TOF) LC/MS systems.
- MassHunter Acquisition for LC/TQ systems 12.0, or higher, which controls and acquires data from Agilent's Tandem Quadrupole (TQ) LC/MS systems.
- MassHunter Quantitative Analysis 11.0 or higher, which is used to quantitatively analyze samples.
- MassHunter BioConfirm 11.0 or higher, which is used to characterize proteins, peptides, and oligos from bio-pharmaceutical sources. This software is optional and may or may not be installed.
- OpenLab ECM 3.5/3.6 which is used for content management and data integrity (LC/TQ systems only).
- OpenLab ECM XT 2.5 or higher which is used for content management and data integrity (LC/TQ, LC/TOF, and LC/Q-TOF systems).

For the purposes of this white paper, MassHunter Networked Workstation will be called MassHunter.

It is the responsibility of the user and their organization to ensure that the technical controls provided by MassHunter are used appropriately to achieve compliance-readiness for laboratory data acquisition and data processing. In addition to the MassHunter technical controls, the user's organization must establish procedural controls--standard operating procedures (SOPs)—to address relevant nontechnical 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 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 Acquisition, it is possible to restrict one user from editing a method, while a different user can create and edit a Worklist. In OpenLab ECM XT content management, user access can be restricted to selected projects. It is possible to restrict a user to only specific information within a specific OpenLab ECM XT 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 predefined 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 Acquisition example. In Figure 1, the Administrator required a reason for saving the acquisition method.

[1] For the context of this white paper, MassHunter Networked Workstation consists of MassHunter Acquisition, MassHunter Quantitative Analysis, and MassHunter BioConfirm installed with the "compliance" toolset and connected with OpenLab ECM XT. The technical controls discussed in this white paper apply to specific versions of each module.

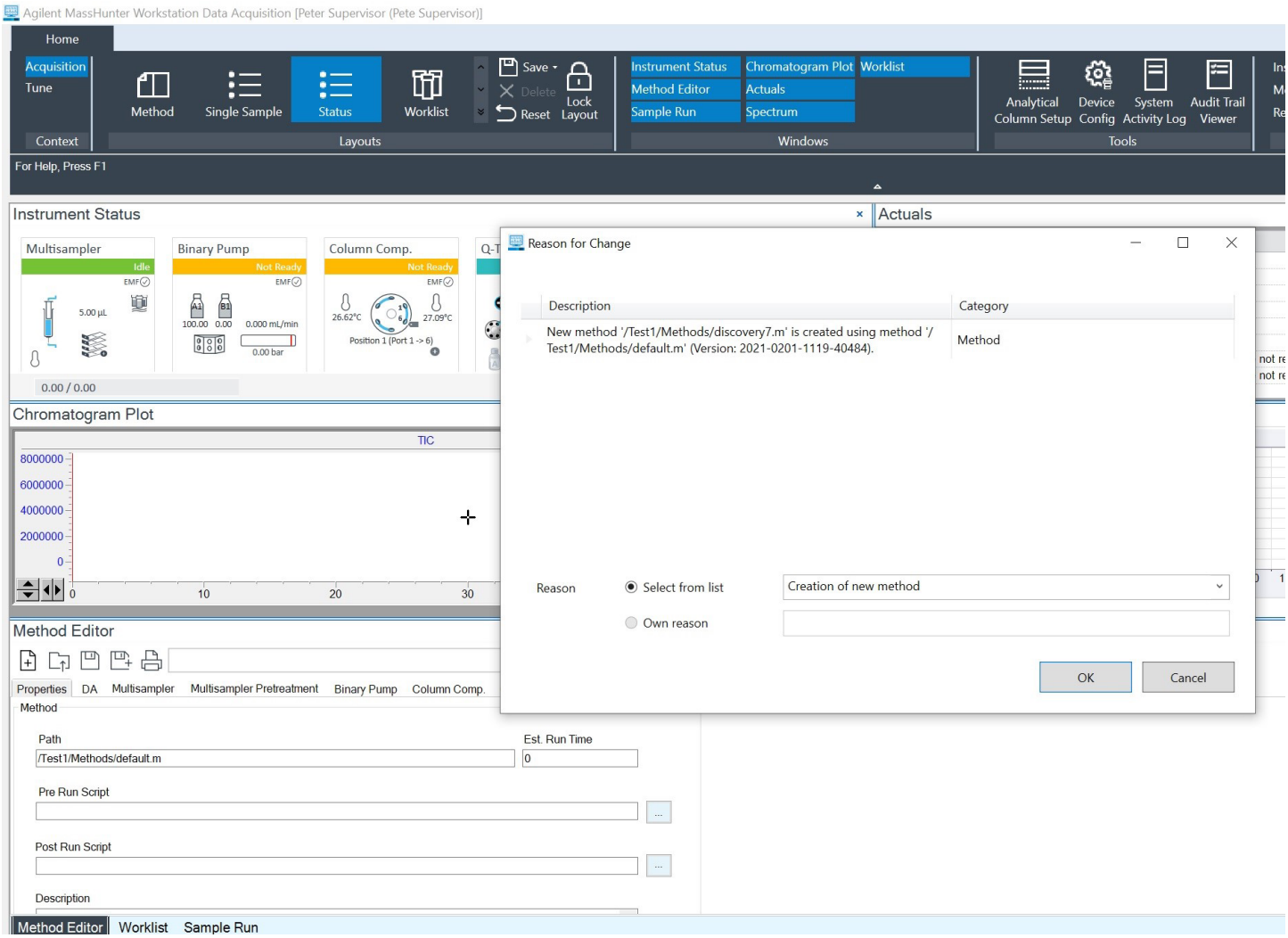

Figure 1. Screenshot of Agilent MassHunter Workstation Data Acquisition showing Reason for Change dialog.

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 a MassHunter Networked Workstation consisting of MassHunter Acquisition, Quantitative Analysis, and BioConfirm revision 11.0 with compliance features activated. Additionally, at a minimum, OpenLab Server or ECM XT 2.5 is required for data integrity when the compliance features are enabled. 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] Other related global requirements are also listed (e.g. Annex 11).

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. Requirements that must be addressed by procedural controls are listed in blue.

Column three

Responsibilities for each requirement are listed in column three. "S" refers to the 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.

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

Table 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. 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.	Yes	Agilent Technologies has extensively verified the performance of MassHunter using tests that evaluate accuracy, reliability, and consistent performance. This statement in no way releases the customer from their regulatory responsibility to validate computerized systems for their intended use. The integrated solution of MassHunter Workstation with OpenLab ECM 3.5/3.6 and OpenLab ECM XT incorporates the use of byte-order dependent checksums at each file transfer operation to ensure that record transfers are valid between the components. The following MassHunter records contain checksum information that can be used to determine if the contents of the associated record component have been altered. With respect to MassHunter, "regulated records" are: – Instrument Tune Parameters – Acquisition Methods – Acquisition Worklists – Acquired Data – Data Analysis Methods - includes Quantitative Analysis and BioConfirm methods – Data Analysis Results - includes Quantitative Analysis and BioConfirm results – Data Analysis Report Templates - includes Quantitative Analysis and BioConfirm report templates – Associated Audit Trails with these records MassHunter check-sums these records to discover any "invalid or altered records." If an invalid or altered record is discovered, an error is displayed and the user is not able to open the file.
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.

Table 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		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) – Quantitative Analysis report templates (V) – BioConfirm report templates (V) – 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 or as provided by ECM XT. 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/TQ, LC/TOF, and LC/Q-TOF LC/MS systems, MassHunter Quantitative Analysis, MassHunter BioConfirm, and OpenLab ECM XT can generate printed copies of all electronically stored e-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?
Brazil	2.3 Are there controls to make sure that the data backup, retrieving and maintenance process is duly carried out?	U	Brazil 585.2	N/A	It is the responsibility of the user organization to control data backup, data retrieval, and maintenance. Detailed instructions are available for creating the appropriate scheduled backup of all relevant files.
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 3.5/3.6 and OpenLab ECM XT. MassHunter stores all raw data, metadata, and result data automatically in OpenLab ECM 3.5/3.6 and OpenLab ECM XT immediately after acquisition, and after each interactive review or automated reprocessing. Data stored in OpenLab 3.5/3.6 and ECM XT reside in a managed, secure storage location. All file actions, including file deletion, are tracked through the OpenLab ECM 3.5/3.6 and OpenLab ECM XT audit trail. All records are protected in the OpenLab ECM 3.5/3.6 and OpenLab ECM XT environment and are retrieved from the OpenLab ECM 3.5/3.6 and OpenLab ECM XT server on review. 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 network connectivity loss, which would initiate a failover mode. It is the user organization's responsibility to manage the physical security and controlled access to OpenLab ECM 3.5/3.6 and OpenLab ECM XT.
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	The system is designed to read data from legacy versions of MassHunter. However, legacy records will not have audit trails or will not be check-summed. 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	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 3.5/3.6 and OpenLab ECM XT has a mechanism to notify admin after a set number of failed login attempts.
Clinical guide	2.8 Are there controls implemented that allow the reconstruction of the electronic source/raw documentation for FDA's review of the (clinical) study and laboratory test results?	S	Clinical Computer Guide F2 FDA Q&As	Yes	All raw data is maintained in secure storage to allow reconstruction of laboratory test results as needed.
Clinical guide	2.9 Does the information provided to 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 performing regular backups of all relevant data?	S	Annex 11.7.1 China GMP 163 Brazil GMP 585 Part 211, 68 b	Yes	OpenLab ECM 3.5/3.6 and OpenLab ECM XT 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.

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?
Clinical Computer Guide	2.12 Are procedures and controls in place to prevent the altering, browsing, querying, or reporting of data via external software applications that do not enter through the protective system software?	S, U	Clinical Computer Guide E	Yes	MassHunter is preconfigured with FTP services enabled to facilitate bulk data operations. Due to the inherent limitations of FTP services, permissions may not be consistent with the permissions granted in MassHunter. Therefore, Agilent recommends disabling FTP services when not needed. See the Administrator's Guide for details.
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?	S, U	Clinical Computer Guide F	N/A	Real time scanning of data being acquired can impact the performance of the instrument. Agilent has tested MassHunter in conjunction with industry standard antivirus applications. However, it is the responsibility of the user organization to implement antivirus software.

Table 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	Each user is identified by a unique ID and password combination. Entry of both is required to access the system.
	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	S, U	Several warning letters	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. It is the user organization's responsibility to ensure unique identities of authorized persons.
Clinical	3.3 Are there controls to maintain a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges?	S, U	Clinical Computer Guide 4	Yes	MassHunter is able to authenticate users via 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 and inherited group privileges. These reports are useful for organizations required to perform periodic security reviews.

Table 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		Yes	MassHunter has a secure, computer-generated, time-stamped activity logs and audit trails for the following records: – Acquisition Method: Yes – Acquisition Worklist: Yes – Acquisition Study Manager: Yes – Acquisition Raw Data: Yes – Instrument Configuration: Yes – MassHunter Quant Results: Yes – MassHunter Quant Method: Yes – MassHunter BioConfirm Methods: Yes – MassHunter BioConfirm Results: Yes – Quantitative Analysis Report Templates: Yes – BioConfirm Report Templates: Yes – OpenLab ECM XT eSignature: Yes – OpenLab ECM 3.5/3.6 eSignature: Yes File actions performed via ECM 3.5/3.6, OpenLab Server, or ECM XT, including file deletion, are tracked through the OpenLab Server or ECM XT 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?
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 the before and after values together with the reason why the change was made. 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. – Acquisition Method: Yes – Acquisition Worklist: Yes – Acquisition Study Manager: Yes – Acquisition Configuration: Yes – MassHunter Quant Batch: Yes, including any changes to the embedded method. – Quantitative Analysis Report Templates: Yes – BioConfirm Report Templates: Yes – MassHunter Quant Method: Yes – MassHunter BioConfirm Methods: Yes – MassHunter BioConfirm Results: Yes
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	Audit trails for records can be printed from any audit trail window. MassHunter Acquisition for LC/TQ, MassHunter Acquisition for TOF and Q-TOF LC/MS systems, MassHunter Quantitative Analysis, MassHunter BioConfirm, and OpenLab Server or ECM XT 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	Audit trails for records can be printed from any audit trail window. MassHunter Acquisition for LC/TQ, MassHunter Acquisition for TOF and Q-TOF LC/MS systems, MassHunter Quantitative Analysis, MassHunter BioConfirm, and OpenLab Server or ECM XT each have this capability.
FDA GMP	4.5 Do such records include the reason for the modification?	S		Yes	The audit trail includes the user ID, date and time of the change, and the before and after values together with the reason why the change was made. 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. – Acquisition Method: Yes – Acquisition Worklist: Yes – Acquisition Study Manager: Yes – Acquisition Configuration: Yes – MassHunter Quant Batch: Yes, including any changes to the embedded method. – MassHunter Quant Method: Yes – MassHunter BioConfirm Methods: Yes – MassHunter BioConfirm Results: 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	Audit trails are always on and cannot be deactivated by any user.
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. Audit trails are readily available in a configurable viewer accessed from the local machine or from a central location. The audit trail viewer indicates which audit trail entries have been reviewed and approved.
	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. MassHunter allows the audit trail to be filtered prior to displaying its contents to address user preferences for reviewing the information.
Part 11 11.10(e)	4.9 Is previously recorded information left unchanged when records are changed?	S		Yes	Records are saved to OpenLab Server or ECM XT. Revisions are created when edits are made, and data is never over-written. OpenLab Server and ECM XT maintains history of all versions of the record. MassHunter audit trails capture old value and new value when records are changed. Changes are stored as new revisions of the original, which is left unchanged. During selection of results for further processing or reporting, the version of the result used can be chosen by the user (based on their permissions).

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)	4.10 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?	S, U		Yes	Audit trail information is stored within the electronic record and cannot be separated from it. MassHunter audit trails are linked with the record and are preserved so long as the record is kept in OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT. OpenLab ECM 3.5/3.6, OpenLab Server, and ECM XT allow 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.
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	MassHunter audit trails can be reviewed and printed.

Table 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?
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. However, it is the responsibility of the user organization to designate and enforce procedural controls as needed.
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 3.5/3.6, OpenLab Server, or ECM XT 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 MassHunter, OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT 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	The identity of operators taking action in the system is recorded in the both the audit trail and activity log.
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 software professionals involved in development of MassHunter have received training in relevant aspects of data integrity.

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(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		N/A	1. It is the responsibility of the user organization to establish systems documentation. 2. Agilent maintains development and testing documentation for the various MassHunter applications, OpenLab ECM 3.5/3.6, OpenLab Server, and OpenLab ECM XT. Upon request, this documentation is available for user review.
Part 11 11.10(l)	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		Yes	It is 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.

Table 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 3.5/3.6, OpenLab Server, or ECM XT 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	Yes	The integrated solution of MassHunter with OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT incorporates the use of byte-order-dependent check-sums at each file transfer operation to ensure that record transfers are valid between the components.
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	Yes	Agilent recommends that the system be configured to reference a time server 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	MassHunter uses the operating system to synchronize with local Windows time. 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 time zone reference used implemented for systems that span different time zones?	S, U	Clinical Computer Guide D.3	Yes	All time data is time stamped in Coordinated Universal Time (UTC)/Greenwich Mean Time (GMT) and displayed in the local time of the computer used.

Table 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?			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?			N/A	MassHunter is not intended to be deployed as an open system as per 21 CFR Part 11.3(b)(9).

Table 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	Yes	The user organization must establish the legal impact of electronic signatures. Signatures are permanently linked to their respective records. Signed electronic records includes the date and time the signature was executed. eSignatures are applied in the OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT client. Signatures are permanently linked to their respective records. They include time and date that they were applied.
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 3.5/3.6, OpenLab Server, or ECM XT 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 3.5/3.6, OpenLab Server, or ECM XT (Native and PDF‡) can be displayed. * Electronic Signatures in PDF are available for printing. ‡ Via eSignature Plug-in for Adobe Acrobat.
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	Handwritten signatures are not addressed by the system and must be managed procedurally by the user's organization. Signed records have a unique checksum that prevents signatures from being excised, copied or otherwise transferred. OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT will not recognize a signature that was applied outside its own electronic signature plug-ins.

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 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 Acquisition for LC/TQ, TOF, and Q-TOF LC/MS systems, MassHunter Quantitative Analysis, and MassHunter BioConfirm support automatic lock-out of a user session after a period of inactivity. The time-out criteria is configured by the administrator. When in the locked state, automated operations within MassHunter Acquisition, such as running a worklist, will continue with appropriate attribution of work. A user must authenticate to retain active control of the system.

Table 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?
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	The system will not allow duplicate user IDs. Each user has a unique login and thus a unique signature that cannot be used by another user. User names in OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT are required to be unique and cannot be reused or reassigned to another individual. Whether OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT uses the company's Windows logins to validate users or OpenLab Server or ECM XT 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	It is the responsibility of the user organization to verify the identify 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, U		Yes	Electronic Signature authentication within OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT 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 3.5/3.6, OpenLab Server, or ECM XT 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 3.5/3.6, OpenLab Server, or ECM XT 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 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 11.200(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 3.5/3.6, OpenLab Server, or ECM XT user executes a series of noncontinuous 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 3.5/3.6, OpenLab Server, or ECM XT 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 3.5/3.6, OpenLab Server, or ECM XT uses the company's domain logins to validate users or OpenLab ECM XT 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.
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	OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT uses the user's user ID and password to initiate the electronic signature. An OpenLab ECM 3.5/3.6 or OpenLab ECM XT user's password is stored encrypted within the database and is displayed as asterisks in all locations within the software. OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT 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. Misuse of electronic signatures by anyone other than the owner would require intentional co-operation of a user and the System Administrator.
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 3.5/3.6, OpenLab Server, or ECM XT do not support biometrics for user authentication.

Table 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	MassHunter authentication can be 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 3.5/3.6, OpenLab Server, or ECM XT uses the company's Windows domain logins to validate users or OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT 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 can use 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 Server or ECM XT 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		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 at their unauthorized use to the system security unit, and, as appropriate, to organizational management?	U		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	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.

Table 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?
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	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	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 with all suppliers (Ref. section 7.4 of the LSCA Quality Manual).
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 with all suppliers (Ref. section 7.4 of the LSCA Quality Manual).
Part 11 11.10(i)	11.5 Is personnel developing and supporting software trained?	S, U		Yes	All Agilent personnel are required to be trained (Ref. section 6.0 of the LSCA Quality Manual).

References

1. Botha, R. A.; Eloff, J. H. P. 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 [Online] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11 (accessed November 19, 2018).

www.agilent.com

RA44239.5716435185

Printed in the USA, May 19, 2022
5994-2902EN

Agilent
Trusted Answers