Support for 21 CFR Part 11 Compliance: Agilent MassHunter for GC/MS

Whitepaper

Overview

US FDA Part 11 in Title 21 of the Code of Federal Regulations (21 CFR Part 11), 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, and accurate, and maintained with integrity.

This white paper is a resource for users of Agilent MassHunter for GC/MS (MassHunter) systems whose organizations must comply with these regulations. MassHunter for GC/MS[1] controls acquisition and processing of single quadrupole GC/MS and triple quadrupole GC/MS systems. It is the responsibility of the user and their organization to ensure that the functionalities provided by MassHunter for GC/MS are used appropriately to achieve compliant operation for laboratory data acquisition and processing. In addition to the technical controls MassHunter for GC/MS provides, the user organization must establish procedural controls--standard operating procedures (SOPs)--to address relevant non-technical requirements. Controls, 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 GC/MS supports users and their organizations in achieving the requirements of each section of 21 CFR Part 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).

Agilent Technologies

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.

For example, in MassHunter GC/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 information within a specific OpenLAB ECM Location and the file access within that location.

> *"Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users."*
>
> *Botha, Eloff, IBM Systems Journal*[1]

1 For the context of this whitepaper, MassHunter for GC/MS consists of MassHunter GC/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.

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 users' actions thus connecting laboratory staff to the work they perform. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

- *Who:* clearly identifies the person responsible for the particular action that creates, modifies, or deletes a record.
- *What:* is the action that took place, including, if applicable, the old value and the new value contained in the record.
- *When:* unambiguously declares the date and time the action took place.
- *Where:* clearly identifies the impacted record.
- *Why:* explains the reason for a change to a regulated record. The reason is often selected from a list of pre-defined reasons to provide consistency and to enable searching and sorting of entries.

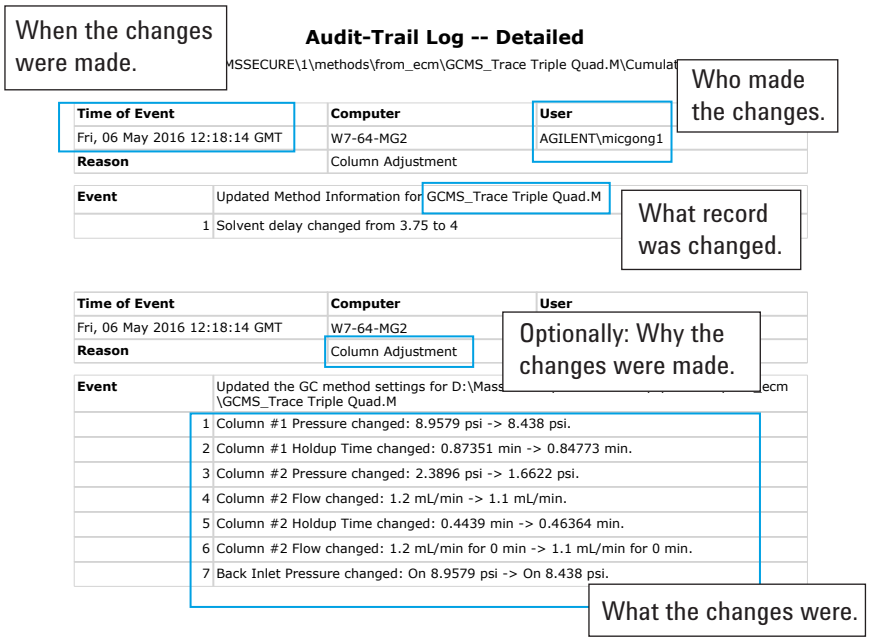
An example of the *Who, What, When, Where,* and (optionally) *Why* can be seen in the MassHunter GC/MS Acquisition example below.

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.



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

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.

Numbering in this document is not necessarily sequential. Gaps in the numeric sequence indicate other regulations that may reviewed by Agilent (for example Annex 11) that are not covered under the scope of this assessment.

Column three

Responsibilities for each requirement are listed in column three. "S" refers to analytical system supplier." "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 GC/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 GC/MS. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 Paragraph	Requirement	Supplier, User	Other regulations or comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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 for shared responsibilities between suppliers and users. While the end user of the system has ultimate responsibility for validation, some tasks can only be done and must be delivered by the supplier, e.g., validation activities during development and related documentation.	Yes[2]	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 our customers 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 Paragraph	Requirement	Supplier, User	Other regulations or comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
Part 11 11.10(a)	**1.1a Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?**			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 Sequences Analysis Methods Analysis Results MassHunter GC/MS Acquisition also validates the integrity of the secured local storage during startup.

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? If no, what is the recommendation?
Part 11 11.10(b)	**2.1 Is the system capable to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying Analysis methods (V and P) 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) Sequences (V and P) Sequence logs (V and P) Audit Trails (V and P) Electronic signatures (V and (all) and P (PDF only)) 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. The metadata stored includes the Tune Report, sequence log, acquisition method, and instrument logbook. This information is considered to be part of the data file record.
Part 11 11.10(c)	**2.4[3] 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, sequences, 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 ECM Audit Trail.

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? 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	A laboratory can control access to MassHunter** and OpenLAB ECM. Only authorized users may use the system, and the lab has the ability to limit certain functionality by user roles. MassHunter GC/MS Acquisition also allows switching the user during operation for the appropriate attribution of work. ** As defined in the scope of this document.
	3.2 Is each user clearly identified, e.g., through 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) – the authorized user is part of the record. It is the laboratories responsibility to ensure unique identities of authorized persons.

4. Electronic Audit Trail

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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	Yes	MassHunter has a secure, computer-generated, time-stamped audit trail for the following records: GC/MS Acquisition Method: Yes†. GC/MS Acquisition Sequence: Yes GC/MS Acquisition Raw Data: Yes GC/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 ECM Audit Trail. †The Sample Prep method and any custom cycle for a PAL autosampler do not have 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 Clinical Computer Guide 2 Clinical Source Data 3	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. GC/MS Acquisition Method: Yes. GC/MS Acquisition Sequence: Yes GC/MS Acquisition Data: Yes GC/MS Acquisition Configuration: Yes MassHunter Quant Batch: Yes, including any changes to the embedded method. * MassHunter Quant Method: No, "**and why**" is not currently available in the Audit Trail.
FDA GMP	4.4 Does the audit trail include any modifications of an established method employed in testing?	S	Part 211.194 8b	Yes	The MassHunter GC/MS Acquisition and Analysis audit trail track changes in the respective methods†. †The current GC/MS Acquisition method audit trail does not include changes in the sample preparation or PAL Custom cycle method elements.

4. Electronic Audit Trail *continued*

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
FDA GMP	4.5 Do such records include the reason for the modification?		Part 211.194 8b	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. GC/MS Acquisition Method: Yes. GC/MS Acquisition Sequence: Yes GC/MS Acquisition Data: Yes GC/MS Acquisition Configuration: Yes MassHunter Quant Batch: Yes, including any changes to the embedded method. * MassHunter Quant Method: No, "**and why**" is not currently available in the Audit Trail.
	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	S,U	Highlighted in at least one Warning Letter	Yes	MassHunter GC/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.
	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	Highlighted in at least one Warning Letter	Yes	Audit Trails are linked to the record – only audit trail entries relevant to the record are viewable when viewing the record.
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. 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 ECM.
Part 11 11.10(e)	**4.11 Is audit trail available for review and copying by the FDA?**	S		Yes	Yes, MassHunter Audit Trails can be reviewed and printed. Refer to the administrator guide for details.

5. Operational and Device Checks

Part 11 and Others	Requirement	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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	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.
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 GC/MS MH Acq / 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. Operational and Device Checks *continued*

Part 11 and Others	Requirement	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
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		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.
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.
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	Is it 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	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		Yes	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 and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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.					

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

Part 11 and Others	Requirement	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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 and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
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 ECM (Native and PDF‡) are capable to 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	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 GC/MS Acquisition, and OpenLAB ECM, can "de-log" the user after a fixed time to a "locked" state. When in the locked state, automated operations within MassHunter GC/MS Acquisition, such as running a sequence, will continue with appropriate attribution of work. A user must authenticate to retain active control of the system. MassHunter Quant Configuration component (ATM) will de-log after 5 minutes of inactivity. * MassHunter Quantitative Analysis does not, at this time, "de-log" the user from the application. This must be addressed by the lab using Procedural Controls.

9. Electronic Signatures General Requirements and Signature Components and Controls

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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	OpenLAB ECM uses the user ID / password combination unique to each user in the electronic signature feature. 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.
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	
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?**	U		N/A	
Part 11 11.100 (c)	**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	
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.

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

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
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.
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 and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? 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.

10. Controls for Identification Codes and Passwords *continued*

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/ No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
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	
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.
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	

11. System Development and Support

Part 11 Others	Requirements	S, U	Other regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied? If no, what is the recommendation?
Part 11 11.10(i)	**11.5 Is personnel developing and supporting software trained?**	S, U	Again joint activity, supplier must have people trained, user should have assurance, e.g., through audit that SW developers are trained and training is documented	Yes	Agilent personnel who develop MassHunter and OpenLAB ECM are made aware of regulatory requirements as appropriate to their function. Agilent provides training to personnel expected to support the software.

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 4, 2015).

www.agilent.com

Published in the USA, May 18, 2016
5991-6909EN

Agilent Technologies