White Paper

Agilent
Trusted Answers

Support for 21 CFR Part 11 and Annex 11 Compliance: ICP-MS MassHunter Workstation Plus Software

Overview

OpenLab Server and ECM XT are ideal compliance solutions for medium to large-sized and expanding laboratories with multiple ICP-MS instruments, while OpenLab ECM is suitable for large laboratories wishing to manage electronic records from multiple instruments and sites. However, the cost and complexity of these server-based compliance solutions may not be appropriate for smaller laboratories that require a simple set of compliance tools to manage records from a single ICP-MS instrument.

For these smaller laboratories, the Agilent ICP-MS MassHunter Workstation Plus software provides a lower-cost route to complying with 21 CFR Part 11 and Annex 11. Workstation Plus is installed on the ICP-MS instrument PC to provide a simple and cost-effective compliance solution for a single Agilent ICP-MS or ICP-QQQ instrument.

In common with OpenLab Server, ECM XT, and ECM integration, the ICP-MS MassHunter User Access Control option uses OpenLab Shared Services (OLSS) functions to control user access to the workstation and record application and workstation audit trails.

Compliance components

Compliance with regulations is a key aspect of an analytical laboratory's operation in many industries, such as pharmaceutical manufacturing, where the principles of good manufacturing practice (GMP) apply.

The four components of compliance related to analytical instruments are:

- Design qualification (DQ), manufacturing quality control, lifecycle management and documentation, and installation and operational qualification (IQ/OQ), for analytical instruments and their software.
- Control of user access to the workstation for instrument control and data processing (restricted user login access with password protection).
- Electronic records security, integrity and traceability (secure storage, file versioning, audit trail, electronic signatures, and archive/retrieval).
- Control of system operation, performance verification (PQ), physical access to the laboratory and associated equipment, Standard Operating Procedures, training and records.

Compliance for Agilent ICP-MS Systems

The first of the compliance components must be demonstrated through the manufacturing quality records and equipment validation certification of the instrument manufacturer.

Design Qualification

Regulated laboratories must ensure that the equipment they use has been designed, manufactured, tested, installed and qualified under an acceptable Quality Process.

In the case of instrument software, this means that the instrument manufacturer must be able to provide a Declaration of Product Validation, to confirm that their software supports user requirements for certification under 21 CFR 58 (Good Laboratory Practice), 21 CFR 210 (Good Manufacturing Practice for Drugs), or 21 CFR 211 (current Good Manufacturing Practice for finished pharmaceuticals). In Europe, the equivalent GxP requirements are covered by ISO standards and ICH guidelines Q8, Q9 and Q10. An example of the Declaration of Product Validation for Agilent's ICP-MS MassHunter software is shown in Figure 1.

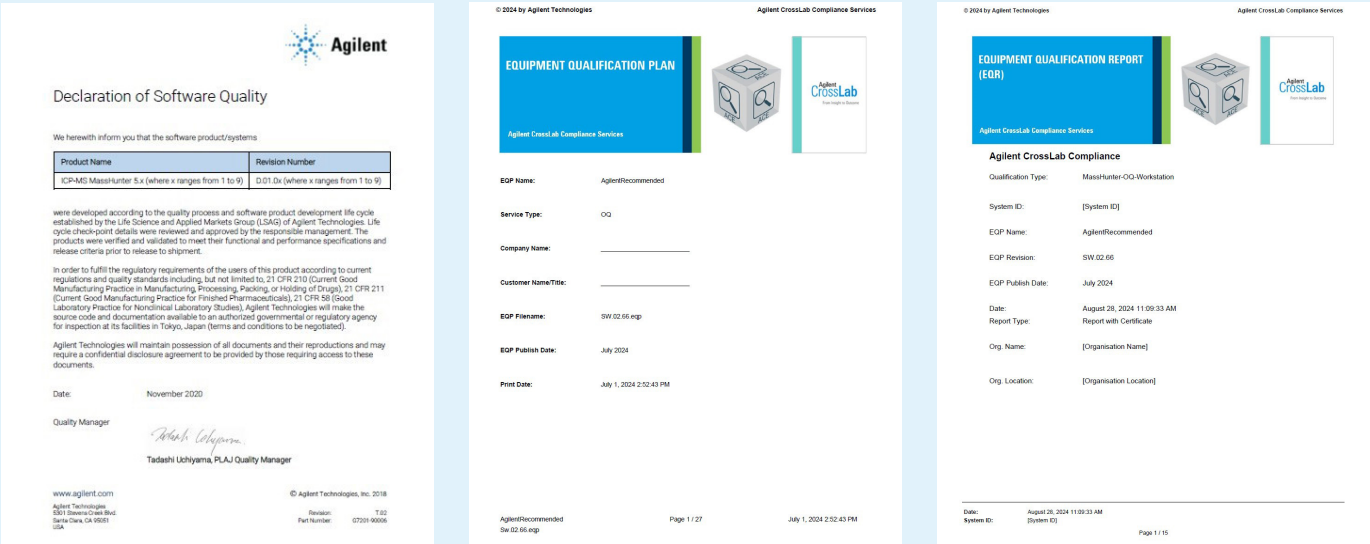


Figure 1. Examples of a Declaration of Software Quality (left) and IQ/OQ qualification report cover sheets.

Installation and Operational Qualification (IQ/OQ)

Once delivered to a user's laboratory, further qualification checks must be carried out, to ensure that the products delivered match the specified items, and that the system hardware and software functions as intended by the manufacturer.

These services are typically performed by the manufacturer and are referred to as Installation Qualification (IQ) and Operational Qualification (OQ). IQ/OQ services, which are often automated, should be available for the instrument system hardware and for all the software components required to operate it. Qualification services will typically include completion of the relevant documentation required to demonstrate compliance with the regulations.

Examples of IQ/OQ document cover sheets for the Agilent ICP-MS hardware and ICP-MS MassHunter software are shown in Figure 1.

Performance and Documentation

To satisfy the fourth component of a complete compliance solution, the responsible personnel in the user organization must set up appropriate controls on laboratory access, ensure that analytical performance is verified for the intended method, and document the procedures to be followed for routine operations.

Once the equipment is installed and qualified, analytical checks, known as System Suitability Testing (SST), are typically performed using the methods and samples that will be measured routinely. SSTs confirm that system performance meets the lab's specific analytical requirements. Agilent has developed a comprehensive standard operating procedure (SOP) which can form part of a complete solution delivered to a laboratory that is setting up pharmaceutical testing according to USP<232> or ICH Q3D. Other related products and services, such as sample preparation equipment and certified calibration standards, can also be supplied to provide an end-to-end, workflow-based approach to setting up the new analytical facility.

User Access and Electronic Records

The remaining two components (system login access and management of electronic records) are typically controlled by software packages which control and monitor user access to the workstation and provide a secure, integrated system for handling the data and other electronic records generated during the lab's activities. These checks are designed to ensure data integrity and are summarized in the ALCOA+ principles, which apply to any records created under GMP controls. ALCOA refers to the fact that records should be Attributable, Legible, Contemporaneous, Original, and Accurate, while the Plus (ALCOA+) added Complete, Consistent, Enduring, and Available.

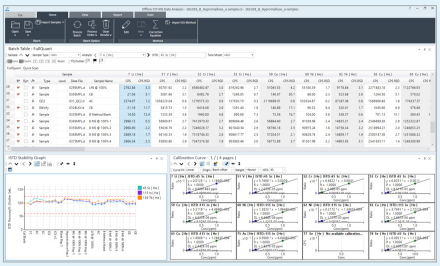
The User Access Control (UAC/OLSS) option for ICP-MS MassHunter supports the user access and data integrity functions, together with one of Agilent's compliance software options: Workstation Plus, OpenLab Basic Server, OpenLab Server, ECM XT, or OpenLab ECM.

ICP-MS MassHunter Workstation Plus

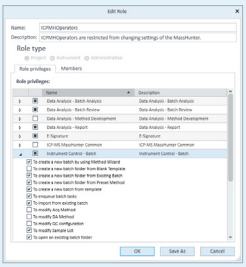
Workstation Plus, in combination with User Access Control, provides compliant operation for Agilent ICP-MS instruments. All software is installed on the standard ICP-MS MassHunter workstation PC, providing a simple and low-cost setup.

Multi-level user access rights and audit trail settings can be configured by the laboratory Administrator, or the default Audit Trail Map (ATM) settings can be used. The ATM settings define which user levels may perform certain functions and whether users must enter a password and reason to verify their access rights for those functions. Database setup and administration is performed through the simple configuration pane.

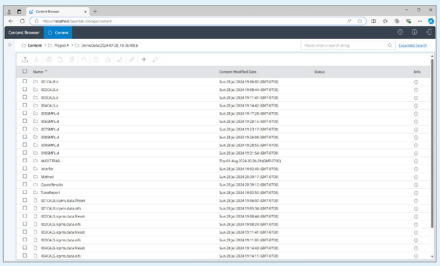
The following table describes how the features and functionality of ICP-MS MassHunter version 5.3 Patch 1 and above, in combination with UAC/OLSS, enables laboratories to meet the regulatory requirements of 21 CFR Part 11, EU Annex 11 and other relevant regulations.



ICP-MS MassHunter
Application software controls the instrument for data acquisition and (re)processing.



User Access Control using OLSS
UAC/OLSS provides security with configurable, multi-level, password protected user profiles. Records user logon/ log-off and actions in audit trail.



ICP-MS MassHunter Workstation Plus
Workstation Plus provides a build-in robust content management system designed to streamline and secure laboratory data handling.

Meeting the Regulatory Requirements of 21 CFR Part 11 with Agilent's ICP-MS MassHunter Workstation Plus software

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
1. Validation			
Part 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?	Yes	Agilent has extensively validated the performance of its systems, including ICP-MS MassHunter Workstation Plus, with tests written specifically to evaluate accuracy, reliability and consistent performance. Agilent recommends making use of the Installation Qualification and Operation Qualification (IQ/OQ) service to validate the onsite system. The use of checksum protection of files uploaded to the secure database storage, version control, and audit trails that show previous and new values support users in implementing systems and procedures to ensure the integrity, security and traceability of their electronic records.
Annex 11.Principle B; Brazil GMP 577	1.2 Is infrastructure qualified?	N/A	User responsibility.
2. Accurate Copies and Secure Retention and Retrieval of Records			
Part 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 by the FDA?	Yes	Raw data, metadata and result data generated by ICP-MS MassHunter Workstation Plus software are handled by the local secure database. ICP-MS MassHunter Workstation Plus reports (e.g. tuning reports and concentration data reports) representing the human-readable form of electronic records can be stored as PDF files which can be printed or made available for review with a PDF viewer without the source application installed on the client machine. These reports can include all data and audit trails.
Annex 11.8.1; Brazil GMP 583	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	Yes	ICP-MS MassHunter Workstation Plus reports (e.g. tuning reports and concentration data reports) representing the human-readable form of electronic records can be stored as PDF files. These files can be printed or made available for review with a viewer without the source application installed on the client machine. These reports can include all data and audit trails.
Brazil 585.2	2.3 Are there controls to make sure that the data backup, retrieving and maintenance process is duly carried out?	Yes	All files stored in the Windows file system or in Workstation Plus can be backed up using the Workstation Plus functionality or with Windows backup utilities. The user organization is responsible for scheduling and performing these backups.
Part 11.10(c); China GMP 163	2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	Yes	Electronic records are automatically saved to the secure database, which is located in Workstation Plus. A user accesses the electronic records. All data files and other regulated records, including audit trails for acquisition and data analysis actions, are also stored in the Workstation Plus database.
Annex 11.17	2.5 Are data checked during the archiving period for accessibility, readability and integrity?	N/A	Functions to check stored data periodically are provided, but using them is the user's responsibility.
Annex 11.17	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?	Yes	Revised software is tested for consistent operation and backward compatibility prior to release. Following the installation of a new or updated revision, Agilent can offer system revalidation as a service.
Annex 11.7.1; Brazil GMP 584	2.7 Are data secured by both physical and electronic means against damage?	Yes	Electronic records are saved and automatically uploaded to the secure database. All data files and other regulated records, including audit trails for acquisition and data analysis actions, are also stored. The user organization is responsible for the physical protection of the PC, data backup, and archival processes.
Clinical Computer Guide F2; FDA Q&As	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?	Yes	All raw data is copied to secure storage to allow reconstruction of laboratory test results as needed. Audit trail entries record the previous and new values for any parameter changed in a method, for example.
Clinical Computer Guide F2; FDA Q&As	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?	N/A	This information is available from the system, but providing it to the FDA is a user's responsibility.
Annex 11.7.1; China GMP 163; Brazil GMP 585; Part 211, 68 b	2.10 Does the system allow performing regular back-ups of all relevant data?	Yes	Tools to support regular backup are provided, but implementation of a data backup system (beyond the e-records in Workstation Plus) is the responsibility of the user organization. Management (e.g. backup scheduling) is also the responsibility of the user organization.
Annex 11.7.1; China GMP 163; Brazil GMP 585; Part 211, 68 b	2.11 Is the integrity and accuracy of backup data and the ability to restore the data checked during validation and monitored periodically?	N/A	Functions to check backed up and restored data are provided, but using them is a user's responsibility.
Clinical Computer Guide E	2.12 Are procedures and controls put 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?	Yes	Electronic records generated by the application are stored in a protected format that cannot be accessed by other software applications. If such a record is altered through another application, it will be detected by the system when trying to read the record.
Clinical Computer Guide F	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?	Yes	Agilent has tested ICP-MS MassHunter Workstation Plus in conjunction with industry-standard anti-virus applications. However, it is the responsibility of the user organization to implement anti-virus software.

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
3. Authorized Access to Systems, Functions, and Data			
Part 11.10(d); China GMP 183 163; Brazil GMP 579; ICH Q7.5.43	3.1 Is system access limited to authorized persons?	Yes	Access to all file and software functionality is controlled by privileges and roles assigned to individual users or groups of users. The system administrator assigns the appropriate level of access to the authorized users or groups. Each user is identified by a unique user ID and password combination. Access to ICP-MS MassHunter Workstation Plus requires entry of a unique identification consisting of a user ID and password.
Several Warning Letters	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	Yes	The system uses a unique user ID and password combination for each user's electronic signature. User IDs must be unique and must not be reused or reassigned to another individual. The organization that implements and uses the system is responsible for this.
Clinical Computer Guide 4	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?	Yes	OLSS User Management and Windows User Account Management functionality includes this information. Maintenance of a cumulative record would be the responsibility of the user organization.
4. Electronic Audit Trail			
Part 11.10(e); China GMP 163	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?	Yes	All actions related to creating, modifying or deleting electronic records are recorded in a secure, computer-generated, time-stamped audit trail. The audit trail lists all modifications, the date and time of the change, the user ID and the reason for the change, if applicable. Entries in the audit trails cannot be switched off, altered or deleted by any user. ICP-MS MassHunter Workstation Plus software automatically generates time-stamped audit trails as a part of electronic records to maintain a complete and accurate history of acquisition and analysis operations. Additionally, Workstation Plus secures audit trail entries for any updates on ICP-MS batches.
FDA 21 CFF 58.130 e; Clinical Computer Guide 2; Clinical Source Data 3	4.2 Does the audit trail record who has made which changes, when and why?	Yes	The audit trail entries contain the name of the user, details of the change made, the date and time, and the reason associated with the signing (if the audit trail map settings specify that a reason is required for the action that triggered the audit trail entry).
Annex 11, 8.2	4.3 Can the system generate printouts indicating if any of the e-records has been changed since the original entry?	Yes	This information is available for method settings via the previous and new values that are recorded in the audit trail entry. Change flags are not supported directly in the ICP-MS MassHunter reports, but Workstation Plus provides version control for records, so version numbers can be used to identify records that have been altered or updated since the original entry.
FDA GMP Part 211.194 8b	4.4 Does the audit trail include any modifications of an established method employed in testing?	Yes	Any change to a method, whether an established method or not, is recorded in the audit trail.
FDA GMP Part 211.194 8b	4.5 Do such records include the reason for the modification?	Yes	The reason for the change to a method is recorded if "reason" is selected for that action in the audit trail map.
FDA Warning Letter	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	Yes	The audit trail function can be configured to be always on. Once it is enabled, only users with administrator privileges to ICP-MS MassHunter can switch it off. So, usual system operators cannot switch it off.
Annex 11, 9	4.7 Is audit trail available to a generally intelligible form for regular review?	Yes	Audit trail records are easily intelligible as the fields and entries stored in the Audit Trail are written in plain language, not specific to ICP-MS MassHunter Workstation Plus functions.
Implicitly required by Annex 11, warning letters (and frequently requested by customers)	4.8 Can audit trail contents be configured such that only relevant activities are recorded for realistic and meaningful review of audit trail information?	Yes	Audit trail contents are nonconfigurable and noneditable by the user. Audit trails an be filtered by user or by entry category. Audit trails can also be searched for each review of entries. Within OpenLab Control Panel, system audit trail content can be filtered prior to displaying its contents to address user preferences for reviewing the information.
Part 11.10(e)	4.9 Is previously recorded information left unchanged when records are changed?	Yes	When new records are added to ICP-MS MassHunter Workstation Plus, both the existing records and the previously recorded audit trial entries are retained. New records are accumulated into the audit trail file. Old records are unchanged at that time.
Part 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?	Yes	The ICP-MS MassHunter Workstation Plus batch audit trail will be retained together with the data for the retention period defined by the user organization.
Part 11.10(e)	4.11 Is audit trail available for review and copying by the FDA?	Yes	Audit trails can be viewed through ICP-MS MassHunter Workstation Plus software. Audit trails and selected entries can be copied or printed using the report function.
Annex 11, 8.1	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?)	Yes	Electronically sorted records including audit trail entries can be printed directly, or copied to printable format.

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
5. Operational and Device Checks			
Part 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?	Yes	Instrument serial numbers are automatically transferred from the ICP-MS instrument to the ICP-MS MassHunter Workstation Plus software. The serial number can be displayed on the software and is recorded in the data file. In addition, the source computer name is recorded for files stored in the database. Prior to data transfer, a device "handshake" confirms the correct link between ICP-MS and the application host computer.
Part 11.10(i); China GMP 18; Brazil 571	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?	Yes	Agilent company policies prohibit disclosure of personal training records. However, audits can confirm the existence of the training program, and materials can state that "Agilent personnel are trained..." Records of the educational and employment history of Agilent Technologies employees are verified and kept with personnel records. End users of ICP-MS MassHunter Workstation Plus are also required to have records of education, training and/or experience with the system at the customer location. Agilent provides a basic familiarization during the installation of the product for system users. Additional system training is available from Agilent.
Part 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?	N/A	User responsibility.
Implied requirement of Part 11 11.10(j)	5.7 Have employees been trained on this procedure?	N/A	User responsibility.
Part 11.10(k); China GMP 161	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?	N/A	User responsibility.
Part 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?	Yes	Agilent's quality and product life cycle processes include formal written revision and change control procedures for system documentation. All controlled document revisions are time-stamped and audit-trailed.
6. Data Integrity, Date and Time Accuracy			
Annex 11.5	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?	N/A	ICP-MS MassHunter Workstation Plus does not exchange data with the other systems.
Annex 11-6; Brazil GMP 580; ICH Q7-5.45	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.)	Yes	Data accuracy and additional checks, such as the validity check of the calibration curve, can be confirmed using appropriate quality control checks, as defined by the user organization. Additional checks can be used, such as reporting confirmatory results for qualifier isotopes. Further checks—such as review by a second operator—are the responsibility of the user organization.
Clinical Computer Guide D.3	6.3 Are controls established to ensure that the system's date and time are correct?	Partial	ICP-MS MassHunter Workstation Plus gets date/time from the operating system, domain controller, or time server (if connected to LAN/WAN). Setting the date/time of the operating system is the responsibility of the user organization and should be controlled using a SoP. Any change to the local OS date/time performed by a user will be recorded in the system audit trail.
Clinical Computer Guide D.3	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?	Partial	ICP-MS MassHunter Workstation Plus gets the date and time from the workstation PC operating system, domain controller, or time server (if connected to LAN/WAN). Only users authorized to access the PC (valid user logon) can access and change the local PC date/time setting. This would be recorded in the system event log, which could be reviewed. Notifications are not sent automatically.
Clinical Computer Guide D.3	6.5 Are time stamps with a clear understanding of the time zone reference used implemented for systems that span different time zones?	Yes	ICP-MS MassHunter Workstation Plus is a single-PC system, so it doesn't span different time zones. The ICP-MS MassHunter Workstation Plus audit trail is recorded with local time + the difference from UTC, such as Thursday, March 01, 2012, 6:52:21 PM (UTC+09:00).
7. Control for Open Systems (Only applicable for open systems)			
Part 11.3	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	ICP-MS MassHunter Workstation Plus is not designed to operate as an open system.
Part 11.3	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	ICP-MS MassHunter Workstation Plus is not designed to operate as an open system.

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
8. Electronic Signatures – Signature Manifestation and Signature/Record Linking			
Annex 11.14; ICH Q7.6.18	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?	Yes	The use and impact of e-signatures within the company are the responsibility of the user organization. Electronic signatures are permanently linked to their respective records and include the date/time (and reason, if required) they were applied.
Part 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?	Yes	Signed electronic records show: 1. The full name and signature level of the signer 2. The date and time the signature was executed 3.The meaning of the signature 4. A comment that is compulsorily entered to indicate the reason for the signature.
Part 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)?	Yes	Electronic signatures applied in ICP-MS MassHunter Workstation Plus software are viewable on the application screen and in printed and electronic reports.
Part 11.7	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?	Yes	Files can be electronically signed in ICP-MS MassHunter software Workstation Plus. The electronic signature is unbreakably linked to the file. The system does not recognize signatures (such as hand-written signatures) that are applied outside its own electronic signature system.
Part 11 Preamble section 124	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?	Yes	ICP-MS MassHunter Workstation Plus has configurable time-based lock functionality, which requires a user login (username and password) to reactivate the application.
9. Electronic Signatures General Requirements and Signature Components and Controls			
Part 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	Yes	The system uses a unique user ID and password combination for each user's electronic signature. User IDs must be unique and must not be reused or reassigned to another individual. The organization that implements and uses the system is responsible for this.
Part 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?	N/A	User responsibility.
Part 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?	N/A	User responsibility.
Part 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?	N/A	User responsibility.
Part 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?	Yes	Both identification (user ID) and password are required to make an electronic signature.
Part 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?	Yes	Both identification (user identification) and password are required to make all electronic signatures.
Part 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?	Yes	Both identification (user identification) and password are required to make all electronic signatures. It is the responsibility of the user organization to ensure the users are not sharing passwords.

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
9. Electronic Signatures General Requirements and Signature Components and Controls			
Part 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?	Yes	Users need to electronically sign each record individually. For each electronic signature, the user must enter two distinct identification components: a unique user ID and password.
Part 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?	Yes	The system 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 manner, the user ID and password combination is known only to the individual. The system also does not allow two users to have the same user ID/password combination. It is the responsibility of the user organization to make sure that user IDs and passwords are used by genuine owners only and are not shared.
Part 11.200(a) (3)	9.10 Are the electronic signatures administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals?	Yes	OpenLab Solutions uses the user's user ID and password to initiate the electronic signature. An application user's password is stored encrypted within the database and is displayed as asterisks in all locations within the software. OpenLab Solutions 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 11.200(b)	9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	N/A	Electronic signatures provided by the system are not based on biometrics.
10. Controls for Identification Codes and Passwords			
Part 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?	Yes	Each user must have a unique user ID and password combination. The user organization is responsible for ensuring that authorized users do not share their account information or access with others. User management is performed in OLSS, which does not allow two individuals to have the same user ID/password combination.
Part 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)?	Yes	OLSS is used for user access management; password renewal intervals can be configured in the OLSS password policy setup. The administrator can define a timeframe in which passwords are periodically revised, automatically. Users are prevented from reusing passwords.
Part 11.300(c)	10.3 Are there procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	N/A	Agilent ICP-MS MassHunter Workstation Plus UAC/OLSS does not use tokens, cards, or other devices, to generate ID codes or passwords.
Part 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?	Yes	The OLSS security policy can be configured so that a user-defined number of unauthorized access attempts locks out the user account, and this can be communicated to a system administrator. The system audit trail documents general events such as logon attempts to the computer as well as application or user changes, in the system event log as a central audit repository for all security information. This includes the system and computer ID along with the operator name and application identification, allowing for an immediate check of any potential security breach. Monitoring and reporting unauthorized use of security information is the responsibility of the user organization.
Part 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?	N/A	Agilent ICP-MS MassHunter Workstation Plus UAC/OLSS does not use tokens, cards, or other devices, to generate ID codes or passwords.

Part 11 or Others	Requirements	Yes/no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
11. System Development and Support			
Annex 11 4.5; Brazil GMP 577; GAMP	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	Yes	Agilent maintains and can provide documented evidence that ICP-MS MassHunter Workstation Plus and UAC/OLSS software are developed under the Quality Management System defined in the current Agilent LSCA Product Lifecycle Revision and ISO QMS certification, together with the documentation for tests performed during product testing and Qualification Services.
Brazil GMP 589	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?	N/A	Agilent ICP-MS MassHunter Workstation Plus software is not developed or supported by using subcontractors.
ICH Q10, 2.7 c	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	N/A	Agilent ICP-MS MassHunter Workstation Plus software is not developed or supported by using subcontractors.

Descriptions taken from 21 CFR Part 11:
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

www.agilent.com/chem

DE-000617

Published in the USA, October 2, 2024
5994-7766EN

Agilent
Trusted Answers