# Meeting regulatory compliance guidelines with Agilent ICP-MS MassHunter and OpenLAB Server

White Paper

## Overview

The United States Pharmacopoeia (USP) and the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) have developed new standards to test for inorganic (elemental) impurities in pharmaceutical products and ingredients: USP General Chapters <232> (Elemental Impurities – Limits) and <233> (Elemental Impurities – Procedures) and ICH-Q3D were finalized in February 2017 and are to be implemented by 1st January 2018. These guidelines specify maximum daily dose limits for the 24 elements listed in Table 1.

ICP-OES and ICP-MS are the reference instrumental techniques for the analysis of Elemental Impurities. ICP-MS is the more suitable technique for analysis of drug products and materials intended for parenteral or inhalational administration, due to the lower detection limits required for such samples.

Agilent Technologies

**Table 1**. USP <232> and ICH Q3D analytes and permitted daily exposure (PDE) limits for drugs intended for oral administration. PDEs for parenteral and inhalational medicines are significantly lower. February 2017 final revision.

| ICH/USP Class | Element | Oral PDE (µg/day) |
|---|---|---|
| Class 1 | Cd | 5 |
| | Pb | 5 |
| | As (inorganic) | 15 |
| | Hg (inorganic) | 30 |
| Class 2A | Co | 50 |
| | V | 100 |
| | Ni | 200 |
| | Tl | 8 |
| | Au | 100 |
| | Pd | 100 |
| | Ir | 100 |
| | Os | 100 |
| Class 2B | Rh | 100 |
| | Ru | 100 |
| | Se | 150 |
| | Ag | 150 |
| | Pt | 100 |
| Class 3 | Li | 550 |
| | Sb | 1200 |
| | Ba | 1400 |
| | Mo | 3000 |
| | Cu | 3000 |
| | Sn | 6000 |
| | Cr | 11000 |

Apart from basic research and drug discovery, all stages of pharmaceutical product development, from pre-clinical assessment to manufacturing Quality Control, are subject to GxP guidelines. These include regulations for electronic data management as defined in Part 11 in Title 21 of the US Food and Drug Administration's Code of Federal Regulations (21 CFR Part 11), the European equivalent (EU Annex 11), PIC/S GMPs, China GMP and the chapter on computer systems of the Brazilian GMP. The purpose of these regulations is to ensure the security, integrity and traceability of electronic records, which includes data, analytical reports and other records (such as daily performance checks) associated with the operation of an analytical instrument.

## Compliance Overview

Regulatory compliance is a key aspect of an analytical laboratory's operation in many industries, especially for pharmaceutical manufacturers. The four components of compliance related to analytical instruments are:

- Design qualification (DQ), manufacturing quality control, lifecycle management and documentation, 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 logon 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

The first of these components must be demonstrated through the manufacturing quality records and equipment validation certification of the instrument manufacturer. In the case of 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).

Once analytical equipment is delivered to the laboratory, further qualification checks must be made to ensure that the products function as defined by the manufacturer. These IQ/OQ services should encompass the instrument hardware and all the software required to operate it, and are typically performed by the manufacturer, Further performance checks are typically performed using the methods and samples that will be analyzed routinely, to confirm that system performance meets analytical requirements.

The fourth component requires that the laboratory manager and administrator set up the appropriate controls on laboratory access, and ensure that system suitability tests (SST) and standard operating procedures (SOP) are documented and followed.

The remaining components—system logon access and management of electronic records—are typically addressed by software packages which control and monitor user access to the workstation, and provide an integrated system for handling the data and other electronic records generated during the laboratory's activities.

## OpenLAB Server

OpenLAB Server is a networked solution for compliant storage of electronic records associated with elemental impurities analysis data acquired with Agilent's ICP-MS MassHunter system. ICP-MS MassHunter is the software that controls Agilent's 7800 and 7900 ICP-MS and 8900 triple-quadrupole ICP-MS instruments.

In addition to storing data from ICP-MS, OpenLAB Server stores data from instruments controlled by OpenLAB CDS. These instrument types include Agilent and non-Agilent LCs and GCs and Agilent. GC/MS and LC/MS single quadrupole systems. OpenLAB Server can manage data from up to 100 instruments.

In combination with an overall laboratory compliance plan, an ICP-MS MassHunter system with OpenLAB Server provides all the technical controls needed to meet 21 CFR Part 11 and Annex 11 requirements.

OpenLAB Server is part of an industry-leading suite of software products designed to integrate and manage scientific information throughout its lifecycle, across the laboratory and the enterprise. OpenLAB Server provides an ideal compliance solution for medium-sized and expanding laboratories. Agilent also offers ICP-MS compliance solutions that are suitable for single-instrument installations (SDA) and global enterprise level organizations (OpenLAB ECM).

## System Overview

The components needed for compliant operation of Agilent ICP-MS instruments with OpenLab Server include: ICP-MS MassHunter software, MassHunter User Access Control (UAC) and OpenLAB Server. Figure 1 illustrates how the components integrate to provide a complete solution.

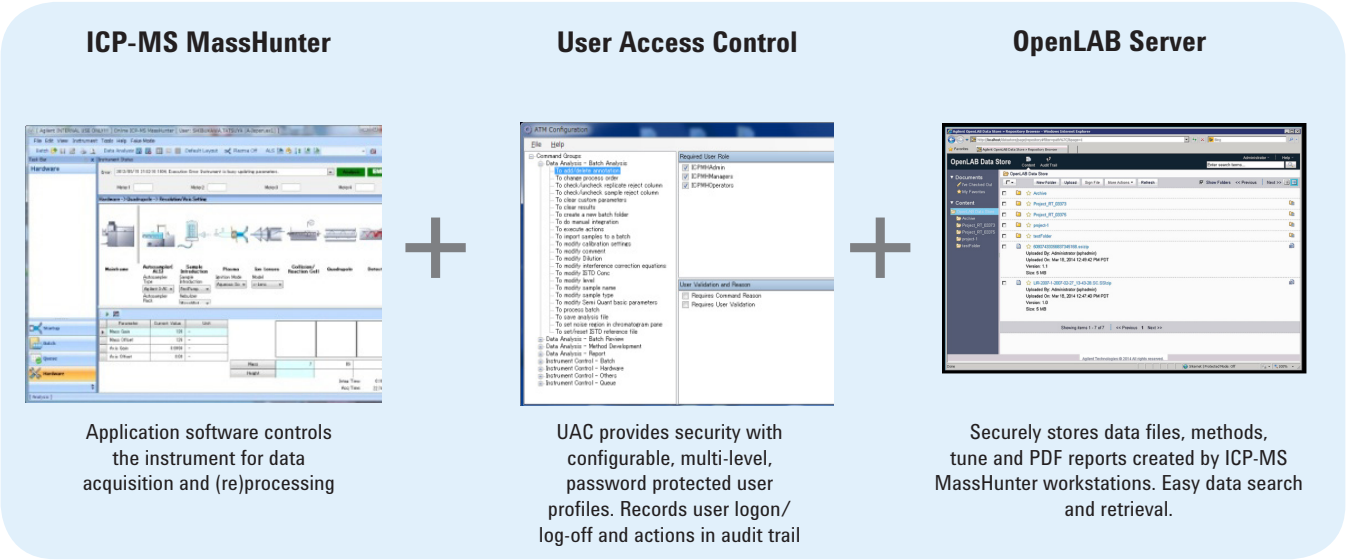


**Figure 1.** Components for compliant operation with ICP-MS MassHunter, User Access Control, and OpenLAB Server

OpenLAB Server integrates with ICP-MS MassHunter and UAC software. All data and reports are stored during the analytical run in a secure data repository, automatically, without user intervention. Any controlled record generated in ICP-MS MassHunter software—tune reports, methods, batches, data files and pdf reports—can be automatically stored in the OpenLAB Server.

With the exception of e-signature capability, OpenLAB Server access is through the MassHunter user interface, allowing data to be easily viewed and downloaded for approval or reprocessing. All raw data, results, methods and reports are kept together, enabling simple access to the original results for auditing throughout the retention period.

## Controlled Access and Audit Trail

A key aspect of electronic records management is control of who is able to access the application software, and what actions they are permitted to perform. For Agilent's ICP-MS MassHunter, this control is provided by the User Access Control module.

Users must login with a unique username and password. Multi-level user access rights and audit trail settings that define the functions users can perform are configured by the Laboratory Administrator. An Audit Trail Map (ATM) ensures that each user is assigned to a role that allows only the actions permitted according to their job and training. Each action can also be setup to require user validation by password and/or reason, and all actions are included in the audit trail. Default ATM settings suitable for a typical laboratory environment are predefined.

As shown in Figure 2, control of user access to the ICP-MS MassHunter workstation and recording of application and workstation audit trails is performed by the MassHunter UAC. Users log-on to the ICP-MS MassHunter Workstation and operate the ICP-MS MassHunter software in exactly the same way as a standalone system, within their level of user access rights.

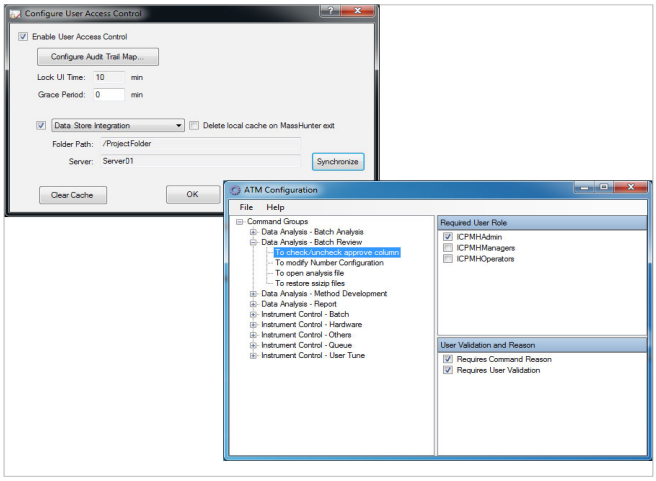


**Figure 2**. Control of user access to the ICP-MS MassHunter workstation, and recording of application and workstation audit trails are performed by the MassHunter User Access Control (UAC) software

## Finding and retrieving data

Data uploaded to OpenLAB Server is securely stored on a suitable server with RAID 1 or RAID 5 architecture (see system requirements on page 11). Data stored on OpenLAB Server is easy to find and retrieve using keyword searching (Figure 3). Records uploaded to OpenLAB Server are automatically indexed so individual records or results can be found easily. As shown in Table 2, Query items such as analyst name, sample acquisition date, and instrument name can be used to find and retrieve individual sample results, or all records for an entire batch. Database setup and administration is performed through OpenLAB Control Panel.

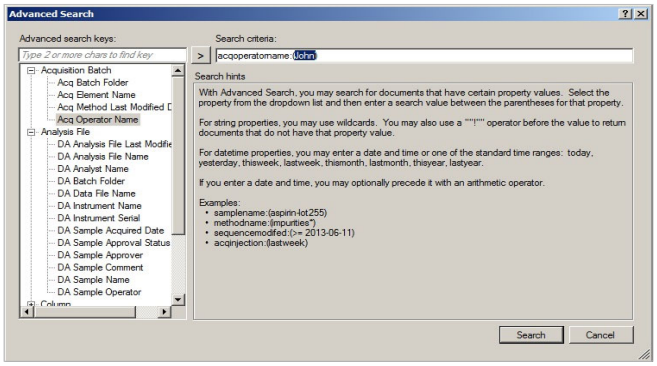


**Figure 3**. OpenLAB Server file retrieval using Advanced Search functions

**Table 2**. Query keys used by OpenLAB Server

| General keys | ICP-MS MassHunter-specific keys |
|---|---|
| File name<br>upload date<br>Sign by<br>Sign date<br>And more | Analyst Name<br>Analysis File Name<br>Analysis File Last Modified Date<br>Batch Folder<br>Data File Name<br>Sample Acquired Date<br>Sample Approval Status<br>Sample Approver<br>Sample Comment<br>Sample Name<br>Instrument Name<br>Instrument Serial<br>Sample Operator<br>Acquisition Batch Folder<br>Acquisition Method Last Modified Date<br>Acquisition Element Name<br>Acquisition Operator Name |

The following tables describe how an ICP-MS MassHunter system with UAC and OpenLAB Server enables laboratories to meet the requirements set forth in 21 CFR Part 11, EU Annex 11 and other related regulations and guidelines.

# Meeting the Regulatory Requirements of 21 CFR Part 11 with Agilent's ICP-MS MassHunter software and OpenLab Server

| Part 11 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| **1. Validation** | | | |
| Part 11<br>11.10(a) and all other regulations | 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 and OpenLAB Server, with tests written specifically to evaluate accuracy, reliability and consistent performance. OpenLAB Server maintains revisions of files as they are modified or altered. The solution also records any and all changes made to the system through computer generated audit trails.<br>Agilent recommends making use of Installation Qualification and Operation Qualification (IQ/OQ) service to validate the on-site system. |
| Annex 11<br>Principle B;<br>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 of generating 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 software are stored and managed in OpenLAB Server. The result set that holds all this information can be loaded at any time to the hard disk of a client PC as a copy of the original data for review. ICP-MS MassHunter software is required to read the electronic format. ICP-MS MassHunter 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 viewer without the source application installed on the client machine. These reports can include all data and audit trails. |
| Annex 11.8.1;<br>Brazil GMP 583 | 2.2 Is it possible to obtain clear printed copies of electronically stored e-records? | Yes | Human readable printed reports are covered in the response to 11.10(b) above. |
| Brazil 585.2 | 2.3 Are there controls to make sure that the data backup, retrieving and maintenance process is duly carried out? | Yes | ICP-MS MassHunter combined with User Access Control software and OpenLAB Server has the capability to backup and retrieve electronic records. It is the user responsibility to ensure such processes are carried out in compliance with the user organization's policy |
| Part 11.10(c):<br>China GMP 163 | 2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period? | Yes | When the compliance software is activated, all regulated, process-related records are automatically stored in the secure OpenLAB Server database. Data secured within OpenLAB Server resides on a protected server. Regardless of the physical location of the data, it remains searchable and retrievable to all users with appropriate privileges. |
| Annex 11.17 | 2.5 Are data checked during the archiving period for accessibility, readability and integrity? | N/A | User 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 prior to release. Following installation of a new or updated revision, system revalidation can be offered as a service delivered by Agilent |
| Annex 11.7.1;<br>Brazil GMP 584 | 2.7 Are data secured by both physical and electronic means against damage? | Yes | OpenLAB Server provides security for electronic records to protect against accidental or malicious damage, and the remote storage (on the OpenLAB server) provides some physical protection. Physical protection of the server (and lab PC), data backup and archival processes are the responsibility of the user organization. |
| Clinical Computer Guide F2;<br>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 | The functionality of the electronic records version control and the change information contained in the audit trail files allow the reconstruction of the original electronic record information. |
| Clinical Computer Guide F2;<br>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 | User responsibility |
| Annex 11.7.1;<br>China GMP 163;<br>Brazil GMP 585;<br>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 remote storage of e-records in the OpenLAB Server system) is the responsibility of the user organization. Management (e.g. backup scheduling) is also the responsibility of the user organization |

| Part 11 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| Annex 11.7.2;<br>China GMP 163;<br>Brazil GMP 585;<br>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 | User 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 | Data is not visible or editable from the lab PC without going through the protective system software. OpenLAB Server's data viewer is also protected via the OpenLAB client logon. |
| 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 implemented controls designed to keep malicious code from being introduced into a regulated customer's systems via any software purchased from Agilent. Physical protection of the computer system from malware (e.g. preventing direct internet connection, and the connection of infected removable storage devices) is the responsibility of the user organization. |
| **3. Authorized Access to Systems, Functions, and Data** | | | |
| Part 11.10(d);<br>China GMP 183 163;<br>Brazil GMP 579;<br>ICH Q7.5.43 | 3.1 Is system access limited to authorized persons? | Yes | All workstation, file and software functionality access 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 with OpenLAB Server requires entry of these unique identification components: 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 user ID and password combination unique to each user in its electronic signature capability. User IDs are required to be unique and must not be reused or reassigned to another individual. This is the responsibility of the organization that implements and uses the system. |
| 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 | 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);<br>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, date and time of the change, the user ID and reason for the change, if applicable. Entries in the audit trails cannot be switched off, altered or deleted by any user. ICP-MS MassHunter UAC 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. OpenLAB Server secures the MassHunter audit trails; in addition it also generates audit trails for any updates on ICP-MS batches. |
| FDA 21 CFF 58.130 e;<br>Clinical Computer Guide 2;<br>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, 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 MassHunter reports that are transferred to OpenLAB Server, but Agilent OpenLAB software can help customers satisfy this requirement via conditional formatting in reports. |
| 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 any 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 any 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 only be switched off (or privileges modified) by a user with appropriate administrator rights. |
| Annex 11, 9 | 4.7 Is audit trail available to a generally intelligible form for regular review? | Yes | The audit trail can be viewed in a tabular format that is easily intelligible. |

| Part 11 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| 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 | The audit trail content is not directly user configurable, but the actions that are recorded in the audit trail are defined in the Audit Trail Map, which enables the user laboratory to choose the actions that require user password and reason |
| Part 11.10(e) | 4.9 Is previously recorded information left unchanged when records are changed? | Yes | Strict security and revision control of the data generated by the ICP-MS MassHunter system is achieved with automatic storage of the result set or single runs in OpenLAB Server after acquisition, automatic reprocessing or any other interactive change. All entries in the ICP-MS MassHunter and OpenLAB Server audit trails are non-editable and non-deletable. Even the removal of records from OpenLAB Server by an authorized user does not affect existing entries in the audit trail. |
| 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 | All audit trail information is stored in the system repository and kept throughout the electronic records retention period. The audit trails are unbreakably linked to the record. System-related activities such as logon events are also unbreakably linked to the system. |
| 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 software or the OpenLAB Server user interfaces. Audit trails and selected entries can be copied to printable format |
| 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 |
| **5. Operational and Device Checks** | | | |
| Part 11.10(f) | 5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required? | Yes | In all functions, when a sequencing of events is required, system checks enforce it. For example, a method cannot be applied to data until the method has been validated for completeness. Users are prompted with an error message when steps are performed out of sequence. |
| Part 11.10(g);<br>Part 211, 68 b | 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? | Yes | Users cannot gain access to the system for acquisition, data processing or review without a valid user name and password. Once logged in, the user's access to files and software functionality (including but not limited to signing a file, inputting values, or altering a record) are determined by their assigned privileges. |
| Annex 11, 12.4 | 5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time? | Yes | ICP-MS MassHunter UAC and OpenLAB Server record this information for actions performed within the application software. For system actions (such as changing the date/time setting), the Windows system event log records the information. |
| 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 | Device identity in the form, of the instrument serial number is transferred from the ICP-MS instrument to the ICP-MS MassHunter software automatically. The serial number can be displayed on software, and it is recorded in the data file. In addition, the source computer name is recorded for files that are uploaded to OpenLAB Server from ICP-MS MassHunter software. Prior to data transfer, a device "handshake" confirms the correct link between ICP-MS and application host computer. |
| Part 11.10(i);<br>China GMP 18;<br>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. Audits can confirm existence of the training program. Materials can state that "Agilent personnel are trained..."<br>Records of the educational and employment history of Agilent Technologies employees are verified and kept with personnel records.<br>End users of ICP-MS MassHunter software with OpenLAB Server 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 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| Part 11.10(k);<br>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? | Yes | The Agilent ICP-MS MassHunter OpenLAB Server system does not exchange data electronically with other systems, apart from connections made to networks or remote drives implemented by the user organization. Data exchanged within the MassHunter OpenLAB environment includes appropriate checks for correct and secure entry. |
| Annex 11-6;<br>Brazil GMP 580;<br>ICHQ7-5.45 | 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 is usually confirmed through the use of 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? | Yes | Date and Time is verified during system setup and qualification. It is the responsibility of the user organization to maintain the correct date and time on the PC system clock |
| 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? | Yes | The date and time settings of the ICP-MS MassHunter workstation PC and OpenLAB Server are only accessible to users with appropriate logon credentials. No external monitoring of system date/time is performed, so confirmation of accurate date/time settings would be the responsibility of the user organization. |
| 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 | Time stamps in normal MassHunter reports show local time, but the audit trail records both local time and UTC, so true times can be referenced and compared for systems that span different timezones |
| **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 | The system 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 | The system is not designed to operate as an open system. |
| **8. Electronic Signatures – Signature Manifestation and Signature/Record Linking** | | | |
| Annex 11.14;<br>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 is the responsibility of the user organization.<br>Electronic signatures are permanently linked to their respective records, and do 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:<br>(1) The printed name of the signer?<br>(2) The date and time when the signature was executed? And<br>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature?" | Yes | Electronic records contain the name of the user, the date and time, and the reason associated with the signing. |
| 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 software are subject to the same controls as for electronic records, and are included in reports that are viewable on the application screen and in printed reports. Electronic signatures applied to ICP-MS MassHunter files in OpenLAB Server are viewable in its details web page and in the file properties dialog box. |

| Part 11 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| 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 | ICP-MS MassHunter files can be electronically signed in ICP-MS MassHunter software and in OpenLAB Server. The electronic signature is unbreakably linked to the file. The system does not recognize signatures (e.g. hand-written) that are applied outside its own electronic signature plug-ins. |
| 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 | A system lock can be applied to ICP-MS MassHunter. This lock requires the re-entry of a valid user's logon credentials to unlock the system computer. |
| **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 user ID and password combination unique to each user in its electronic signature capability. User IDs are required to be unique and must not be reused or reassigned to another individual. Management of this process is the responsibility of the organization that implements and uses the system. |
| 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 | The electronic signature tools require two distinct identification components prior to applying signatures on files: A unique user ID and password. |
| 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 | Users need to electronically sign each record individually. For each electronic signature, the user has to enter two distinct identification components: A unique user ID and password. |
| 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 | Users need to electronically sign each record individually. For each electronic signature, the user has to enter two distinct identification components: A unique user ID and password |
| 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 has to 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.<br>The system also does not allow two users to have the same user ID / password combination. It is the responsibility of the organization to make sure that user IDs and passwords are used by genuine owners only and are not shared. |

| Part 11 or Others | Requirements | Yes/No | If yes, how, specifically, is the requirement satisfied, or if no, what is the recommendation to customers? |
|---|---|---|---|
| Part 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? | Yes | Both user IDs and passwords are kept unique to users. The system administrator only knows user IDs when setting up users. At each user's first logon, they must define their unique password which is only known to them. Thus attempted use of an individual's electronic signature by others requires active collaboration with the purpose of sharing passwords. |
| 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 used with ICP-MS MassHunter and OpenLAB Server are not based upon 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 | Identity management is performed in Windows User Account manager and OpenLAB control panel 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 | Using Windows domain authentication, password renewal intervals can be configured in 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. |
| 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 | User responsibility |
| 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 Windows security policy can be configured so that a user defined number of unauthorized access attempts locks out the user account and sends email notification 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 Windows 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 the potential security leak. |
| 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 | User responsibility |
| **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 aqnd OpenLAB Server software is developed under the Quality Management System defined in Agilent LSCA Product Lifecycle Revision D.05 and ISO9001-2008, and described in the 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 software is not developed or supported using subcontractors. |
| ICHQ10, 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 software is not developed or supported using subcontractors. |
| ICHQ10, 2.7 c | 11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined? | N/A | Agilent ICP-MS MassHunter software is not developed or supported using subcontractors. |

Descriptions taken from 21 CFR Part 11:
www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11

## System Requirements

Agilent OpenLAB Server is a server-based system that is scalable from a single to 100-concurrent-instrument implementation. Instruments operating with Agilent ICP-MS MassHunter or Agilent OpenLAB CDS are supported. The recommended server specifications for up to two ICP-MS systems are shown in the table below. OpenLAB Server requires a database backend and supports either PostgreSQL or Microsoft SQL Server 2012 SP2.

### Recommended system configuration for OpenLAB Server running on a single server configuration

| Hardware | Medium system | Large sized system |
|---|---|---|
| | (3-30 logical instruments*) | (31-100 logical instruments*) |
| Processor | 2 × (Intel Xeon E5 v2 | 2 × (Intel Xeon E5 v3 |
| | 2.5 GHz, 4 Core) | 3.0 GHz, 4 Core) |
| Minimum Ram | 24 GB | 48 GB |
| Disk (OS and software) | 2 × (300 GB 15 K rpm RAID 1) | 2 × (600 GB 15 K rpm RAID 1) |
| Disk (Data)** | 3 × (500 GB 7.2 K rpm RAID 5) | 5 x (1 TB 7.2 K rpm RAID 5) |
| Network | 1 GB | 1 GB |
| **Software** | | |
| Operating system for OpenLAB Server system | | |
| OpenLAB Server server: | Windows Server 2012 R2 Standard or Enterprise Edition | |
| OpenLAB Server client: | Windows 7 SP1 (64-bit) Professional or Enterprise Edition | |
| | Windows 10 (64-bit) Professional or Enterprise Edition | |
| | Windows Server 2012 R2 Standard or Enterprise Edition | |
| | MS SQL Server 2014 SP2 | |
| **Databases** | | |
| Agilent OpenLAB Server manages information using a database. The database is installed and configured either manually or automatically during installation. | | |
| Supported database software: | SQL Server 2012 Standard or Enterprise (64-bit) SP2 | |
| | PostgreSQL Server 9.3 | |
| | Oracle 12c R1 | |

* 1 ICP-MS instrument counts as 2 logical instruments. For full information see OpenLAB Server Hardware and Software Requirements Guide (M8440-90021, April 2017)

** The disk space recommendation is based on estimated requirements for four years' operation. Actual disk space requirements should be calculated for the lab's intended usage patterns

**www.agilent.com/chem/**



Published May 4, 2017
Publication number: 5991-2593EN

**Agilent Technologies**