Support for 21 CFR Part 11 and Annex 11 Compliance: SDA module for Agilent ICP-MS MassHunter software

White paper

Overview

Part 11 in Title 21 of the US Code of Federal Regulations (commonly referred to as 21 CFR Part 11) governs food and drugs in the US, and includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The equivalent guidelines in the European Union are defined in EU Annex 11.

The purpose of these regulations is to ensure the security, integrity and traceability of electronic records, which includes method information, data, analytical reports and other records (such as daily performance checks) asssociated with the operation of an analytical instrument.

Agilent's 7800 and 7900 Series ICP-MS and 8900 ICP-QQQ instruments are controlled by ICP-MS MassHunter software. ICP-MS MassHunter supports integration with Agilent's Spectroscopy Database Administrator (SDA), OpenLAB Server or ECM (Enterprise Content Manager) software to provide users with the tools to ensure compliance with FDA, European and other relevant guidelines relating to the handling of electronic records.

Agilent Technologies

OpenLAB Server is an ideal compliance solution for medium-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. But 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, Agilent's Spectroscopy Database Administrator (SDA) software provides a lower cost route to complying with 21 CFR Part 11 and Annex 11. SDA (which is also compatible with Agilent's ICP-OES instruments) is installed on the ICP-MS instrument workstation 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 and ECM integration, the control of user access to the ICP-MS MassHunter workstation and recording of application and workstation audit trails is performed by ICP-MS MassHunter's User Access Control option.

Overview

Compliance with regulations is a key aspect of an analytical laboratory's operation in many industries, especially pharmaceutical manufacturing

The 4 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

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 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 finshed 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.

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 should be available for the instrument system hardware and for all the software components required to operate it.

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.

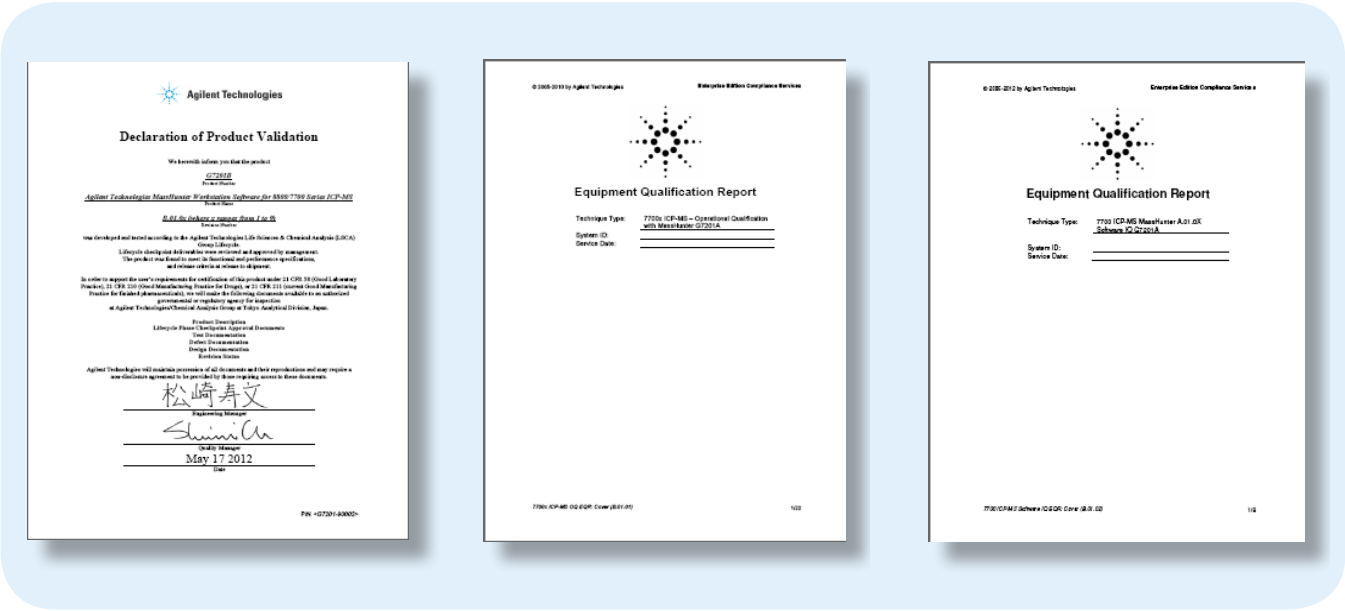


Figure 1. Examples of a Declaration of Production Validation (left) and IQ/OQ qualfication report cover sheets

User Access and Electronic Records

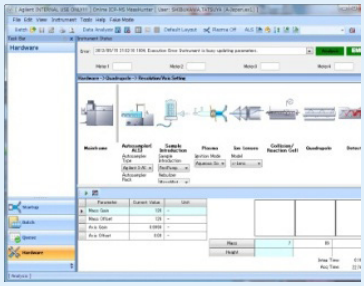
The remaining 2 components (system logon access and management of electronic records) are typically controlled by software packages which control and monitor user access to the workstation, and provide a secure, integrated system for handling the data and other electronic records generated during the lab's activities.

These functions are supported by the User Access Control (UAC) option for ICP-MS MassHunter, together with one of Agilent's three compliance software packages: SDA, OpenLAB Server, or OpenLAB ECM.

ICP-MS MassHunter with SDA

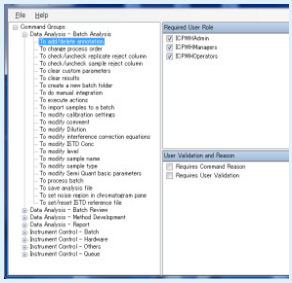
The components of the ICP-MS MassHunter/UAC/SDA software system that provides compliant operation for Agilent ICP-MS instruments are illustrated below. All software is installed on the standard ICP-MS MassHunter workstation PC, providing a simple and low-cost setup.

ICP-MS MassHunter



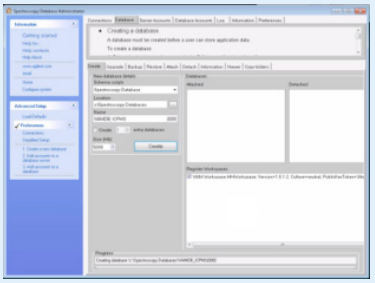
Application software controls the instrument for data acquisition and (re)processing

User Access Control



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

SDA Software ICP-MS MassHunter Version



Databases are created by SDA and accessed by the application software. SDA uses Microsoft® SQL Server® 2008 R2 Express Edition

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 SDA configuration pane.

The table (following) describes how the features and functionality of ICP-MS MassHunter, in combination with UAC and SDA, enables laboratories to meet the regulatory requirements of 21 CFR Part 11, EU Annex 11 and other relevant regulations.

Meeting the Regulatory Requirements of 21 CFR Part 11 with Agilent's ICP-MS SDA 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 and SDA, with tests written specifically to evaluate accuracy, reliability and consistent performance. Agilent recommends making use of Installation Qualification and Operation Qualification (IQ/ OQ) service to validate the on-site system. The use of checksum protection of files uploaded to the secure SDA 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 software are copied into and managed in SDA. The result set that holds all this information can be transferred 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; Brazil GMP 583	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	Yes	ICP-MS MassHunter software is required to read the electronic format files. 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.
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 SDA can be backed up using SDA functionality or with Windows backup utilities. Scheduling and performing these backups is the responsibility of the user organization.
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	With SDA in Protect Local Data mode, electronic records are saved and automatically uploaded to the secure SDA database. A user accesses the electronic records which are located in SDA. All data files and other regulated records, including audit trails for acquisition and data analysis actions, are copied to SDA.
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; Brazil GMP 584	2.7 Are data secured by both physical and electronic means against damage?	Yes	With SDA in Protect Local Data mode, electronic records are saved and automatically uploaded to the secure SDA database. All data files and other regulated records, including audit trails for acquisition and data analysis actions, are copied to SDA. Physical protection of the PC, data backup, and archival processes is the responsibility of the user organization.
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 records 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	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 users?
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	All files stored in the Windows file system, including data exported from SDA, can be backed up with ordinary Windows backup utilities.
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	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?	Partial	Acquisition data, reports and associated method files are secured by transfer to SDA database. These records cannot be viewed or altered outside of the application software. Prevention of unauthorized user access to the workstation PC and its files must be implemented via user organization SOPs. Any attempt to modify or delete such records would be visible in the system event log.
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 and SDA in conjunction with industry standard anti-virus applications. However, it is the responsibility of the user organization to implement anti-virus software.
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	All 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 SDA 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	This requirement can be satisfied via integration with Windows user management and Active Directory services.
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, 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. SDA can secure the MassHunter audit trails once they are uploaded; in addition SDA generates audit trail entries for any updates on uploaded 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, 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?	Partial	Change 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 MassHunter reports but version numbers indicate whether a record has 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.

Part 11 or Others	Requirements	Yes/ no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
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 the audit trail function is enabled, only users who has administrator privilege to ICP-MS MassHunter can switch it off. So usual system operators cannot switch it off. The audit trail log for SDA Administrator can be viewed in SDA Administrator.
Annex 11, 9	4.7 Is audit trail available to a generally intelligible form for regular review?	Partial	Each ICP-MS MassHunter batch can have its own audit trial file, so audit trail records are easily intelligible. The fields and entries stored in the Audit Trail are considered to be easily intelligible for an appropriately trained person familiar with ICP-MS MassHunter functions. The audit trail log for SDA Administrator is also reasonably intelligible.
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?	Partial	Contents of the Audit Trail are not directly configurable, as all user actions are recorded. However, a filter function is available to allow entries to be located more easily. Regarding audit trail for SDA Administrator, the log can be viewed in SDA Administrator. The log can be filtered.
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, 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. Regarding audit trail for SDA Administrator, the log can be viewed in SDA Administrator. The log is accumulative.
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	Audit trail records for ICP-MS MassHunter and SDA are stored in SDA. The ICP-MS MassHunter batch audit trail will be retained together with the data, for the retention period defined by the user organization. Regarding audit trail for SDA Administrator, the log can be viewed in SDA Administrator. It can be archived in the local disk and viewed throughout the retention period or as defined by the user organization.
Part 11.10(e)	4.11 Is audit trail available for review and copying by the FDA?	Yes	ICP-MS MassHunter audit trail file is xml file. So agency can copy it and reviewing it by any XML viewer. Regarding audit trail for SDA Administrator, the log can be viewed in SDA Administrator.
Annex 11, 8.1	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?)	Partial	E-audit trail can be printed as a representation (copy) of the UI display. Others records such as hardware configuration, acquisition method, and data analysis method and quantitation results can be printed clearly. Regarding audit trail for SDA Administrator, the log can be viewed in SDA Administrator. The log can be printed and exported to xml file.
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	If sequencing of events is required, system checks enforce it. For example, before batch (sample analysis sequence) is executed, the batch must be validated and saved, otherwise, the batch cannot be executed.
Part 11.10(g); 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	Audit trail records the identity of operators entering, changing, confirming or deleting data including date and time. Regarding SDA, the log can be viewed in SDA Administrator. The log works for this purpose.
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 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 SDA 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 or Others	Requirements	Yes/ no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
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. Audits can confirm existence of the training program. 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 software with SDA 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 with SDA doesn't 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 validity check of calibration curve can be 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?	No	ICP-MS MassHunter gets date/time from the operating system. Setting the date/time of the operation system is the responsibility of the user organization and should be controlled using a SoP. Any change to the OS date/time performed by a user would 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 and SDA get the date and time from the workstation PC operating system. Only users authorized to access the PC (valid user logon) can access and change the PC date/time setting. This would be recorded in the Windows 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 with SDA is a single-PC system so it doesn't span different time zones. MassHunter audit trail is recorded with local time + difference from UTC such as Thursday, March 01, 2012, 6:52:21 PM (UTC+09:00). SDA stores information regarding the time zone
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 with SDA 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?
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 with SDA is not designed to operate as an open system.
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 is the responsibility of the user organization. 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: (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	Electronic records created by ICP-MS MassHunter and SDA contain the name of the user, the date and time, and the reason associated with the signing (if selected in the Audit Trail Map).
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 viewable on the application screen and in printed reports. SDA can display e-signature which is applied to an electronic record.
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. 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 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	ICP-MS MassHunter has a time-based lock functionality requiring a user logon (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 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.
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 or Others	Requirements	Yes/ no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
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 a 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. 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 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 provided by the system 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	Each user must have a unique user ID and password combination. It is the responsibility of the user organizatio to ensure that authorized users do not share their account information or access with others. Identity management is performed in Windows user management 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	Windows authentication is used for user access management; 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 or Others	Requirements	Yes/ no	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
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 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	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 and SDA software is 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 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 software is not developed or supported by using subcontractors.
ICH Q10, 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 by using subcontractors.

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

www.agilent.com/chem/

Published December 20, 2017
Publication number: 5991-2002EN

Agilent Technologies