# Integration of the Agilent ChemStation for GC, LC, LC/MSD, CE, CE/MSD and A/D with Agilent OpenLAB ECM - Compliance with 21 CFR Part 11

Technical Note

## Introduction

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures.

The intent of these guidelines is to ensure that applicable electronic records are reliable, authentic and maintained with high integrity. This technical note describes features and functionality of Agilent ChemStation for GC, LC, LC/MSD, CE, CE-MSD, and A/D, version B.04.01 or higher, in combination with Agilent´s OpenLAB Enterprise Content Manager for data management, which enable them to meet the guidelines of 21 CFR part 11.

This document examines each section of 21 CFR Part 11 and provides a recommended remediation approach using:

- The Agilent ChemStation B.04.01 with the G2189BA ChemStation OpenLAB option
- The Agilent OpenLAB Enterprise Content Manager (further on referred to as Agilent ChemStation OpenLAB ECM integration) for electronic records management.

The G2189BA ChemStation OpenLAB option for the Agilent ChemStation B.04.01 provides a tight and seamless integration into OpenLAB ECM. The ChemStation OpenLAB option adds the necessary controls for managing system access, data transfer handling and audit trail functionality, while Agilent OpenLAB ECM ensures secure record keeping, and data archival, and grants user privileges for ChemStation users.

Agilent OpenLAB ECM is proven to satisfy compliance needs as mandated by regulations such as 21 CFR Part 11. It has been implemented by many leading life science companies for this reason.

## 21 CFR Part 11 sections addressed by the Agilent ChemStation OpenLAB ECM integration [ChemStation revision B.04.01 higher]

**Applicable sections of 21 CFR Part 11 for ChemStation operated in a closed system**

| Possible scenarios with ChemStation operated in a closed system | 11.1, 11.2, 11.3 | 11.10 | 11.30 | 11.50 | 11.70 | 11.100 | 11.200 (a) | 11.300 (a), (b), (d) | 11.300 (c), (e) |
|---|---|---|---|---|---|---|---|---|---|
| Electronic Record only (without signature) | √ | √ | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Electronic signature based upon user ID and Password | √ | √ | N/A | √ | √ | √ | N/A | √ | N/A |

The G2189BA Agilent ChemStation OpenLAB option in combination with the Agilent OpenLAB ECM data management solution enables the operation of the Agilent ChemStation in full support of all compliance requirements mandated by 21 CFR part 11 for a closed system. In particular it ensures:

- Accurate and complete copies of records
- Versioning of all relevant records for traceability
- Preservation of records between their creation and their automatic transfer to Agilent OpenLAB ECM immediately after acquisition, reprocessing or interactive modifications
- Controlled copies of the data
- Mandatory login to Agilent OpenLAB ECM before allowing access to the ChemStation
- Records of changes captured in user-independent time-stamped audit trails

These settings can be configured during or after installation to meet your specific standard operation procedures and security guidelines. This includes granular ChemStation user roles and privileges providing restricted access to ChemStation functionality for particular users. Changes to the configuration can be done at any time by a dedicated system administrator. Details and recommendations for configuration of the system are outlined in the manual "ChemStation OpenLAB option”, Part Number G2170-90233, available on the Agilent ChemStation Installation DVD or on the Agilent website.

The Agilent ChemStation OpenLAB integration was not specifically designed for operation in an open system.

**NOTE:** In this technical note the term "ChemStation" (in the context of integration with OpenLAB ECM) always refers to the ChemStation revision B.04.01 or higher with a license for the ChemStation OpenLAB option installed and the respective feature set enabled.

| 11.10 Controls for Closed Systems | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.10(a) | Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records? | Yes. Agilent develops its products according to the well established "product lifecycle" concept, which is a phase review process for software and hardware development, to ensure consistent product quality. As a result, a fully qualified data handling system is delivered with all necessary services needed to implement such a system in order to meet the requirements of the FDA regarding 21CFR Part 11. As part of the installation and qualification services, a protocol is compiled that describes the installed configuration and documents the results of the executed IQ and OQ procedures.<br>Electronic records generated by ChemStation are securely stored in Agilent OpenLAB ECM. Agilent OpenLAB ECM's performance has been extensively validated with tests written to specifically evaluate accuracy, reliability and consistent performance. Agilent OpenLAB ECM incorporates the use of byte-order dependent check sums at each file transfer operation to ensure that records are valid and unaltered. |
| 11.10(b) | Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA? | Yes. Electronic records are created in electronic as well as human-readable form.<br>OpenLAB ECM centrally stores all data types, from raw machine data to printable reports. All files are unaltered and stored in the original format. Raw, meta and result data generated by ChemStation are stored and managed in Agilent OpenLAB ECM. The data container 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. The Agilent ChemStation is required to read the electronic format. "Printed" reports, representing the human-readable form of electronic records, can be stored as PDF files which can be made available for review without the source application installed on the client machine. These reports can include all data and audit trails. Viewers are available to view the original electronic record without the original application. |
| 11.10(c) | Are the records protected for accurate and convenient retrieval throughout the record retention period? | Yes. Raw, meta and result data generated by the Agilent ChemStation are stored and managed in Agilent OpenLAB ECM.<br>The data resides in a protected storage location or archive media or both. When archived, the media may be on-line, near-line or off-line. Regardless of the physical location of the data, it remains searchable to all users with appropriate privileges. The individual users do not need access to the physical storage location of the files.<br>The ChemStation can be configured to store all raw, meta and result data automatically in Agilent OpenLAB ECM immediately after acquisition and after each interactive review or automated reprocessing.<br>The functionality is complemented by additional procedural controls that should be defined and implemented by the system administrator based on company-wide security policies. These policies should manage practices such as access to client computers and password renewal frequency. |
| 11.10(d) | Is system access limited to authorized individuals? | Yes. Each user is identified by a unique user ID and password combination.<br>Logging on to the Agilent ChemStation requires the entry of both identification components to gain access to the system. As part of the system configuration, this logon can be enforced as mandatory for all users. Access to data maintained in Agilent OpenLAB ECM is controlled by the need to provide a user name, password, and account login. Once a user has authenticated himself successfully, all file and software functionality access is controlled by privileges and roles assigned to individual users or groups of users. The system administrator determines levels of access.<br>In addition to ECM-specific privileges in ECM user administration, a set of more than 40 ChemStation privileges is available to allow limited system access to authorized individuals and control the access level of different user roles. These privileges can be combined when defining individual user roles. The ChemStation access privileges offer granular access restriction to ChemStation functionality. The system offers four pre-defined user roles for ChemStation access levels. User and role management is handled in ECM, where user management can be integrated with Windows user management. Depending upon access restrictions, menu items, graphical elements or views in the ChemStation can be enabled or disabled. |

| 11.10 Controls for Closed Systems | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.10(e) | Is there a secure, computer-generated audit trail that independently records 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 name and reason for the change if applicable. Entries in the audit trails cannot be switched off, altered or deleted by the user.<br>The ChemStation OpenLAB ECM integration ensures that all meta data is stored along with raw data and result data. This ensures the sequence container and single run concepts of ChemStation to maintain full data integrity. When a sequence or single run is initiated, the methods and the sequence template associated with the run(s) are copied to the data container or single run. The stored information includes all audit trails related to the result data and the method(s) used for data generation. All changes to a running sequence or single run are captured as well.<br>The Agilent ChemStation OpenLAB ECM integration provides three types of audit trails:<br>*1. OpenLAB ECM Audit Trail*<br>The OpenLAB ECM audit trail records who has accessed the system and what operations he or she has performed during a given period of time. The recorded activities include items such as data storage, versioning, and electronic signatures. Removing records from the database does not affect existing entries in the audit trail. Logon and logoff to the ChemStation, as well as user changes, are similarly documented.<br>*2. Method Audit Trail*<br>The method audit trail consists of two components:<br>a) the method management concept which saves used methods along with the data files, introduced with ChemStation Revision B.02.01<br>b) the method audit trail<br>The method audit trail tracks all changes to the data acquisition and data analysis parameters. The system enforces user-added comments for any changes to the data acquisition parameters. Any changes to the data analysis parameters are automatically tracked with the user name, date and time of the method modification, and user comments. The audit trail documents the changes from one "save" to the next.<br>*3. Results Audit Trail*<br>A result-specific audit trail contains a log of changes that occurred when a user worked on one revision of a run. Manual integration activities and changes are actively saved to the data file and the logbook tracks all result changes from one "save" to the next. Manual integration is automatically tracked with the user name, date and time, and performed steps of the integration modification.<br>In addition, the OpenLAB ECM system log keeps a record of all revisions to the OpenLAB ECM system, including configuration edits, e-mail notifications, and additions or changes of locations, cabinets, drawers, or folders. |
| 11.10(e) | When records are changed, is previously recorded information left unchanged? | Yes. The combination of audit trails and strict revision control ensures that previous information is not obscured.<br>All entries in the audit trails are non-editable and non-deletable. Even the removal of records from Agilent OpenLAB ECM by an authorized user does not affect existing entries in the audit trail.<br>Strict revision control of the data generated by the ChemStation is achieved by forcing automatic storage of the sequence containers or single runs in OpenLAB ECM after acquisition, automatic reprocessing or any other interactive change. Records are securely stored in a protected transfer queue that cannot be accessed by unauthorized users. This prevents any alteration of records between their creation or modification in ChemStation and storage in OpenLAB ECM as may occur, for example during a network outage. |

| 11.10 Controls for Closed Systems | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.10(e) | Are electronic audit trails saved at least as long as their subject electronic records and available for agency review and reproduction? | Yes. All Agilent OpenLAB ECM audit trail information is stored in the OpenLAB ECM repository as part of a file´s meta data and kept throughout the electronic records retention period. The OpenLAB ECM audit trails are unbreakably linked to the record, or the system for system-related activities such as logon events.<br>The results audit trail is part of the run logbook and is stored with each data file. The method audit trail is part of the method and is stored with each method file. Both, data file and method are stored in OpenLAB ECM. This ensures an unbreakable link between record and related audit trail. |
| 11.10(f) | Are operational system checks used to enforce permitted sequencing of steps and events? | Yes. In all ChemStation B.04.01 and Agilent OpenLAB ECM functions, when a sequencing of events is required, system checks enforce it.<br>A few examples are:<br>• A process that requires sequenced steps is the archive or delete procedure. In Agilent OpenLAB ECM, record retention policies can be set up to ensure the controlled deletion of records at the end of the record retention period. These record retention policies include review and arbitration procedures. Agilent OpenLAB ECM provides an optional Business Process Manager (BPM), which allows sequencing of practices such as electronic signatures in an approval process.<br>• If only approved methods are to be used in QA/QC, this can be achieved by restricting user access to the approved methods stored in Agilent OpenLAB ECM.<br>• In ChemStation, Agilent uses a clear prerun/run/postrun structure in its 'Run Control' functionality to ensure proper sequencing of steps.<br>• The ChemStation user privileges managed in OpenLAB ECM combined with the ChemStation ECM preferences are both entirely managed by a system administrator and restrict the user to an automatic transfer of the records from ChemStation to Agilent OpenLAB ECM. This ensures that ChemStation records are always stored in OpenLAB ECM. |
| 11.10(g) | Are authority checks in place 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 current operation? | Yes. Users cannot gain access to Agilent OpenLAB ECM without a valid user name, password and account. The ChemStation B.04.01 can be configured to enforce a mandatory login to OpenLAB ECM.<br>Only a successful logon to the system offers access to files and general software functionality, chromatographic software functions or archival and approval functionality. This includes file signing, value input, record alteration, and other practices. The user must authenticate with a valid user name, password and account. This applies at program initiation and after every inactivity timeout on the computer program. User access to specific functionality in the software is further restricted by the privileges assigned to the individual user. These privileges can be combined into roles if necessary. |
| 11.10(h) | Are device checks used to determine, as appropriate, the validity of the source of data or operational instruction? | Yes. For ChemStation, instrument serial numbers are transferred electronically (for example, 1200 HPLC or 7890 GC). This is completed automatically from the instrument. The instrument serial number is recorded in the ChemStation full report, and in the ChemStation ACAML[1] file, both of which can be stored with the ChemStation results in ECM. An OQPV must be executed to ensure that devices and software are functioning properly.<br>User entry fields in ChemStation provide feedback to the user about the entry types and ranges that are valid for a particular field. |
| 11.10(i) | Do the persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks? | Yes. Records of the educational and employment history of Agilent employees are verified and can be made available during an on-site audit. In addition, all Agilent Technologies employees who work with regulations have attended training workshops for regulatory requirements.<br>Agilent provides a basic familiarization during the installation of the product for system users. Training courses for administrators as well as users are available. |

[1] The ACAML file format is an Agilent standard designed for the documentation and exchange of meta and result data.

| 11.10 Controls for Closed Systems | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.10(j) | Have written policies that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification been established and followed? | N/A. It is the responsibility of the organization implementing electronic signatures to develop written policies to ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature. |
| 11.10 (k)(1) | Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance? | N/A. While documentation is available for Agilent ChemStation OpenLAB option and OpenLAB ECM for users and administrators, controls over the storage and distribution of this material are the responsibility of the organization that implements and uses the system. |
| 11.10 (k)(2) | Are there formal revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation? | Yes. The quality process includes written formal revision and change control procedures for system documentation. Agilent OpenLAB ECM can be used for development and maintenance of system documentation. An audit trail of all revisions to the documents is maintained and time-stamped. |

| 11.30 Controls for Open Systems | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.30 | Are there procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt? | Yes. When a file is transferred to or within Agilent OpenLAB ECM, a byte-order dependent checksum is calculated on the file in its source location. A copy of the file is made in the destination location where a second checksum is calculated. The two values are compared and if they are identical, the transfer is complete. If the values do not match, an error message is generated.<br>The Agilent ChemStation OpenLAB integration was not specifically designed for operation in an open system. |
| 11.30 | Are additional measures used to ensure the confidentiality of the electronic records from the point of their creation to the point of their receipt? | Yes. Agilent OpenLAB ECM supports the use of Secure Socket Layer (SSL) encryption for security during data transmission. SSL breaks a single file into very small data packets. These data packets are individually encrypted with configurable 64-bit or 128-bit encryption before being transmitted. On the receiving side the data packets are decrypted and reassembled. ChemStation OpenLAB Option supports SSL encryption.<br>The Agilent ChemStation OpenLAB integration was not specifically designed for operation in an open system. |

| 11.50 Signature Manifestation | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.50(a) | Do the signed electronic records contain information associated with the signing that clearly indicates the following:<br>• printed name of signer<br>• date and time that the signature was executed<br>• meaning associated with the signature? | Yes. The ChemStation data container or SSIZip file can be electronically signed in ECM. Agilent OpenLAB ECM's electronic signature manifestation includes:<br>• User name in addition to the full name of the signer<br>• Signer's title<br>• Date and time that the signature was applied<br>• Location where the signing occurred<br>• User configurable meaning associated with the signature<br>The eSignature Plug-in for Adobe Acrobat places a visible signature manifestation on all human readable forms of the document, electronic display and printed form. |
| 11.50(b) | Are these items part of any human readable form of the electronic record? | Yes. The eSignature Plug-in for Adobe Acrobat places a visible signature manifestation on all human readable forms of the document, electronic display and printed form. Note that PDF documents cannot be signed if they are part of a ChemStation data container, or SSIZip file. |

| 11.70 Signature/Record Linking | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.70 | Is the electronic signature linked to its respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means? | Yes. The ChemStation data container (SSIZip file) can be electronically signed in OpenLAB ECM. The electronic Signature is unbreakably linked to the file. The eSignature Plug-in for Adobe Acrobat encrypts the signature within the document to prevent the signature from being excised or copied to another document. Agilent OpenLAB ECM will not recognize a signature that was applied outside its own electronic signature plug-ins. |

| 11.100 Electronic Signatures: General Requirements | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.100 (a) | Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else? | Yes. Agilent OpenLAB ECM uses the user ID and password combination unique to each user in the electronic signature feature. User names within Agilent OpenLAB ECM are required to be unique and cannot be reused or reassigned to another individual. |
| 11.100 (b) | Are the identities of the individuals verified prior to the establishment, assignment, and certification of an individual's electronic signature or any element of an electronic signature? | N/A. This is the responsibility of the organization that plans, implements and operates the system. Such a verification process is a system requirement that is set before implementing electronic signature procedures or assigning electronic signature privileges to an individual. |
| 11.100 (c) | Has the company delivered its corporate electronic signature certification letter to FDA? | N/A. It is the company's responsibility, before submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature. |
| 11.100 (c)(2) | Is it in paper form with a traditional handwritten signature? | N/A. This is the responsibility of the organization that operates the system. See 11.100(c). |
| 11.100 (c)(2) | Can additional certification or testimony be provided so that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature? | N/A. This is the responsibility of the organization that operates the system. See 11.100(c). |

| 11.200 Electronic Signature Components and Controls | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.200 (a)(i) | Does the e-signature employ at least two distinct identification components such as user ID and password? | Yes. The Agilent OpenLAB ECM electronic signature tools consist of two components: unique user ID and password. |
| 11.200 (a)(1)(i) | When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components? | Yes. When an individual signs the first of a series of documents during a single period of controlled access, the user is required to enter both signature components: user ID and password. |
| 11.200 (a)(1)(i) | When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual? | Yes. When an Agilent OpenLAB ECM user executes a series of continuous electronic signatures, which are defined as signatures executed within period of time determined by the system administrator, they are required to enter user ID, password and reason with the first signature only. Each subsequent signature requires only the user's password, which is known only to the user. |
| 11.200 (a)(1)(ii) | When an individual executes a series of signings not performed during a single, continuous period of controlled system access, does each signing executed require all signature components? | Yes. When an Agilent OpenLAB ECM user executes a series of non-continuous electronic signatures, which are defined as signatures executed outside of a system administrator determined period of time, they are required to enter user ID, password and reason with each signature. |
| 11.200 (a)(2) | Are controls in place to ensure that only their genuine owners can use the electronic signature? | Yes. Agilent OpenLAB ECM can be configured such that an administrator can assign an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this manner the user ID and password combination is known only to the individual. |
| 11.200 (a)(3) | Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals? | Yes. Agilent OpenLAB ECM applies the user ID and password to initiate the electronic signature. An Agilent OpenLAB ECM user's password is stored encrypted within the database and is displayed as asterisks in all locations within the software.<br>The system administrator is aware of user IDs when he installs the users. During installation he can force a password change during the first logon. This password is only known to each user as it is defined during the first logon. See also 11.200(a)(2). The enforcement of this policy is the responsibility of the organization that operates the system. Therefore, it requires active collaboration with the purpose of sharing passwords to enable irregular use of another users’ identification.<br>Agilent OpenLAB ECM can be configured so that an administrator can assign an initial password to a user for new account or forgotten password, but the user is required to change that password on their first login. |
| 11.200 (b) | Are electronic signatures based on biometrics designed to ensure that only their genuine owners can used them? | N/A. Agilent OpenLAB ECM does not support signatures based on biometrics at this time. |

| 11.300 Controls for Identification Codes/Passwords | | |
|---|---|---|
| **Section** | **Question** | **Agilent ChemStation OpenLAB ECM integration** |
| 11.300<br>(a) | Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password? | Yes. Agilent OpenLAB ECM requires users to authenticate with user ID and password. Agilent OpenLAB ECM uses the company's Windows NT logins as well as OpenLAB ECM IDs and passwords to validate users. Therefore no two users can have the same user ID and password combination. |
| 11.300<br>(b) | Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised? | Yes. Password renewal interval is configured as part of the Windows password policy setup. The administrator can define a time frame in which passwords are periodically revised automatically. Users are prevented from reusing passwords.<br>Agilent OpenLAB ECM can also be configured so that user passwords are periodically revised automatically and users are prevented from reusing passwords. |
| 11.300<br>(c) | Are there loss management procedures in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information? | N/A. Neither Agilent OpenLAB ECM nor ChemStation support devices that bear or generate identification codes, such as tokens or cards, at this time. |
| 11.300<br>(d) | Are transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes? | Yes. The system can be configured so that only the user knows their user ID and password identification code. Passwords are always displayed as asterisks and are stored encrypted within the database so that even an administrator cannot see them. |
| 11.300<br>(d) | Are transaction safeguards in place 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. Agilent OpenLAB ECM can be configured so that a user-defined number of unauthorized access attempts locks out the user account and sends an email notification to a system administrator.<br>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. |
| 11.300<br>(e) | Are there controls in place to initially test devices 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. Neither Agilent OpenLAB ECM nor ChemStation support devices that bear or generate identification codes, such as tokens or cards, at this time. |

www.agilent.com/chem/cds

June 1, 2009
Publication Number 5990-4075EN

Agilent Technologies