White Paper

Agilent OpenLab

Support for Title 21 CFR Part 11 and Annex 11 compliance: Agilent OpenLab EZChrom version A.04.10 with OpenLab ECM

Overview

US FDA Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its EU analog, Eudralex Chapter 4, Annex 11, describe the requirements for electronic records and electronic signatures for regulated pharmaceutical organizations. Released in 1997, 21 CFR Part 11 has been enforced since 1999. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with integrity.

This white paper is a resource for users of Agilent OpenLab EZChrom version A.04.10 and OpenLab ECM systems whose organizations must comply with these regulations. OpenLab EZChrom controls acquisition and processing of LC, GC, and A/D data. It is the responsibility of the user and their organization to ensure that the functionalities provided by OpenLab EZChrom are used appropriately to achieve compliant operation for laboratory data acquisition and processing. In addition to the technical controls OpenLab EZChrom provides, the user organization must establish procedural controls–standard operating procedures (SOPs)– to address relevant non-technical requirements. For example, controls such as internal audit programs, must also be established to ensure that system operators follow the SOPs.

Appendix 1 provides a detailed description of how OpenLab EZChrom version A.04.10 supports users and their organizations in achieving the requirements of each section of 21 CFR Part 11 and the related sections of EU Annex 11. The descriptions assume that system access, including instrument hardware and software, is controlled by the staff responsible for the electronic records contained on the system. Thus, the system is designed as a "closed system" as defined in 21 CFR Part 11.3(b)(4).

Agilent

Trusted Answers

21 CFR Part 11 covers three specific elements of a regulated laboratory's operation:

- Security of electronic records,
- Attribution of work,
- Electronic signatures (if used)

Security

Security can be interpreted as "the right people, having the right access, to the right information." Regulated organizations must be able to both verify the identity of system users and limit system access to trained, authorized individuals (11.10(d), (i) and (g); 11.100(b)). Because laboratory staff have different responsibilities based on their job assignments, data access must be segregated and defined such that certain users have certain types of access to certain sets of data while potentially having different access to other data sets.

Attribution of work

Attribution of work refers to documenting the "Who, what, when, where and why?" of work performed. Automated audit trails independently record users actions thus connecting laboratory staff to the work they perform. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

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

eSignatures

While 21 CFR Part 11 does not require the use of eSignatures, it does provide regulations for their use when they are used. In this case, the system must ensure that eSignatures:

- Are irrevocably linked to their respective records.
- Show the full name of the signer, date and time, as well as the meaning of, or reason for, the signature (such as review, approval, responsibility, or authorship).
- Are present whenever the signed records are displayed or printed.

"Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users."

– Botha, Eloff, IBM Systems Journal[1]

Appendix 1. Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations using OpenLab EZChrom with OpenLab ECM.

Appendix 1 Table: Notes

Column one

The table addresses 21 CFR Part 11 requirements in the order that they are presented in the US FDA reference document. [2] Related requirements such as those found in EU Annex 11[3] follow each section of Part 11.

Column two

For completeness, column two lists all requirements of 21 CFR Part 11 and other related global requirements. "System" refers to the analytical system used to acquire and process data.

Most requirements are fulfilled by either technical controls (i.e., software functionality) or procedural controls (i.e., SOPs). Technical controls are controls provided by the software and hence the software supplier, while procedural controls are the responsibility of the user organization. 21 CFR Part 11 requirements listed in bold are requirements addressed by technical controls. Other global requirements are listed in regular font. Requirements that must be addressed by procedural controls are listed in blue.

Column three

Some requirements involve both technical and procedural controls. Responsibilities for each requirement are listed in column three. "S" refers to analytical system supplier. "U" refers to the user organization. Rows containing requirements that must be exclusively addressed by the user organization are shown in blue. Blue may also be technical controls the user will be responsible to implement.

Column four

If available and where appropriate, related global requirements and comments are provided in column four.

Column five

Column five indicates with a "yes" or "no" whether the requirement can be satisfied using the technical controls provided in OpenLab EZChrom or OpenLab ECM. N/A is not applicable to OpenLab.

Column six

Column six explains how the regulatory requirement can be satisfied using the technical controls provided by OpenLab EZChrom or OpenLab ECM. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 and Others	Requirements	S, U	Other associated regulations and comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(a)	1.1 Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S, U	Required by all regulations This is a typical example for shared responsibilities between suppliers and users. While the user firm has ultimate responsibility for validation, some tasks can only be done and must be delivered by the supplier, e.g., validation activities during development and related documentation. Pay particular attention to the technical requirement regarding discernment of "invalid or altered records." 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。	Yes	Agilent Technologies has extensively verified the performance of OpenLab EZChrom using tests that evaluate accuracy, reliability and consistent performance. However, the user organization is required to validate their analytical system according to regulatory expectations. With respect to Agilent OpenLab EZChrom, "regulated records" are: – Analytical methods – Acquired data – Analysis results – Report Templates – Sequence Associated audit trails ▯ Method Audit trail ▯ Sequence Audit trail ▯ Data Audit trail ▯ Result Set Audit trail ▯ Advance Report Audit trail ▯ Sample prep Audit trail – Electronic signature (applicable to data inside the result set) OpenLab EZChrom with ECM has the ability to flag /identify invalid or alter record through check-sums and if a new file is entered in the same location then a revision of that file is created.
Annex 11	1.2 Is infrastructure qualified?	U	Annex 11. Principle B Brazil GMP 577	N/A	Qualification of infrastructures, such as servers and networks, is the responsibility of the user organization.

2. Accurate Copies and Secure Retention and Retrieval of Records

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(b)	2.1 Is the system capable to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA?	S	第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （一）为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。	Yes	The following electronic records can be exported in human readable form and in electronic form for the regulator for review: – All Reports – All Audit trails – Instrument Activity logs – Chromatogram(s) – Graphics export Records are available printed on paper or electronically as a PDF file.
Annex 11	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	S	Annex 11.8.1 Brazil GMP 583	Yes	Records are available printed on paper or electronically as a PDF file.
Brazil	2.3 Are there controls to make sure that the data backup, retrieving and maintenance process is duly carried out?	S, U	Brazil 585.2 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （三）应当建立数据备份与恢复的操作规程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	No	OpenLab EZChrom has the ability to back up the contents of the project folder including the Results, Method, Sequence, Sample prep and Template using 3rd party tools into a Safe external location. It is the responsibility of the user organization to restore the data from the external location into OpenLab EZChrom.
Part 11 11.10(c)	2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	S, U	China GMP 163	Yes	All the metadata is stored in the ECM DB and physical files (raw data & result data) is stored on a physical device. It is the user organization responsibility to manage the physical security and controlled access to the workstation and the servers.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability and integrity?	U	Annex 11.17	N/A	It is the responsibility of the user organization to ensure data are checked during archival for accessibility, readability, and integrity.
Annex 11	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?	S, U	Annex 11.17	Yes	The system is designed to read data from legacy versions of OpenLab EZChrom. The user organization is responsible for ensuring readability of this data during their implementation and validation processes.
Annex 11	2.7 Are data secured by both physical and electronic means against damage?	S, U	Annex 11.7.1 Brazil GMP 584 第五章系统 第十条系统应当安装在适当的位置，以防止外来因素干扰。 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如 计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。	Yes	It is the customer's responsibility to prevent physical damage to hardware that generates and retains data. It is also the customer's responsibility to implement backup and disaster recovery mechanisms. Electronically, data is secured by controlled access via authentication and authorization. Secured communication protocols between OpenLab EZChrom and ECM are used to protect data transfer between system components. ECM has a mechanism to notify admin after a set number of failed login attempts.

2. Accurate Copies and Secure Retention and Retrieval of Records *continued*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Clinical guide	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?	S	Clinical Computer Guide F2 FDA Q&As	Yes	OpenLab EZChrom with ECM can open the original Raw data files in the source system when needed for FDA review.
Clinical guide	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?	U	Clinical Computer Guide F2 FDA Q&As	N/A	It is the responsibility of the user organization to describe how source/raw data were obtained and managed, and how electronic records were used to capture data.
Annex 11	2.10 Does the system allow performing regular back-ups of all relevant data?	S	Annex 11.7.1 China GMP 163 Brazil GMP 585 Part 211, 68 b	Yes	OpenLab EZChrom has the ability to allow secured back up of all relevant data using 3rd party tools. OpenLab ECM has facilities to allow for the administrator to perform periodic backups of the database. However, it is user organization responsibility to perform regular back up of the data and check the accessibility, readability, and integrity.
Annex 11	2.11 Is the integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically?	U	Annex 11.7.2 China GMP 163 Brazil GMP 585 Part 211, 68 b	N/A	It is the responsibility of the user organization to ensure the integrity and accuracy of the backed-up data, and also to check, validate and monitor restored data periodically.
Clinical Computer Guide	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?	S,U	Clinical Computer Guide E	Yes	Data is only accessible through OpenLab EZChrom. No external application can connect to ECM without proper credentials and access to data is protected by user access control
Clinical Computer Guide	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?	S,U	Clinical Computer Guide F	Yes	Agilent has tested OpenLab EZChrom in conjunction with industry standard anti-virus applications. However, it is the responsibility of the user organization to implement anti-virus software and keep it up to date.

3. Authorized Access to Systems, Functions, and Data

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(d)	3.1 Is system access limited to authorized persons?	S, U	China GMP 183 163 Brazil GMP 579, ICH Q7.5.43	Yes	OpenLab EZChrom has ability to create unique user ID and password for each user however it is user organization responsibility to configure these users.
	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	S, U	Several Warning Letters	Yes	OpenLab EZChrom has ability to uniquely identify each user with the combination of user ID and password.
Clinical	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?	S, U	Clinical Computer Guide 4	Yes	OpenLab EZChrom is able to authenticate users via either the Windows Domain or locally in the application itself. Access privileges are set in the Shared Services and any changes are recorded in the activity log. Reports are available that show users' individual and inherited group privileges. These reports are useful for organizations required to perform periodic security reviews.

4. Electronic audit trail

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(e)	4.1 Is there a secure, computer-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records?	S	China GMP 163 第五章系统 第十六条计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改一个已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结果，考虑在计算机化系统中建立一个数据审计跟踪系统，用于记录数据的输入和修改。	Yes	All user activities are recorded in secure, computer generated, time-stamped audit trails. Audit trails are created for all result data, methods, and sequences.
FDA GLP	4.2 Does the audit trail record who has made which changes, when and why?	S	FDA 21 CFF 58.130 e Clinical Computer Guide 2 Clinical Source Data 3	Yes	Audit trail in OpenLab EZChrom has the ability to record user actions with the user ID, date and time of the change including the before and after values with the reason for change. OpenLab ECM audit trail has the ability to record the user ID, date and the time, the description of the change along with the reason.
Annex 11	4.3 Can the system generate printouts indicating if any of the e-records has been changed since the original entry?	S	Annex 11, 8.2	Yes	In OpenLab EZChrom the changes to the records (data, method, sequence, sample prep, advance report and result) are recorded in audit trails (Data audit trail, method audit trail, sample prep audit trail, sequence audit trail, advance report audit trail and result audit trail). These audit trails can be exported to PDF and printed.
FDA GMP	4.4 Does the audit trail include any modifications of an established method employed in testing? 4.5 Do such records include the reason for the modification?	S	Part 211.194 8b	Yes	In OpenLab EZChrom changes to the method are recorded in method audit trails which also includes reasons for method modification.

4. Electronic audit trail *continued*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	S,U	Warning Letter	Yes	OpenLab EZChrom has the ability to enforce Global audit trail to be always ON, by enabling GATE (Global audit trail Enforcement) functionality during the initial installation however it is user organization responsibility to enable this function.
Annex 11	4.7 Is audit trail available to a generally intelligible form for regular review?	S	Annex 11, 9	Yes	In OpenLab EZChrom the audit trails are readily available for review in the audit trail tab with a configurable filter to view. In OpenLab ECM audit trails the data is readily available for review from file property.
	4.8 Can audit trail contents be configured such that only relevant activities are recorded for realistic and meaningful review of audit trail information?	S	Implicitly required by Annex 11 and many warning letters related to review of audit trail. Strong customer request	No	In OpenLab EZChrom allows the audit trail to be filtered to address user preferences for reviewing the information. All the events that are recorded in the audit trail is preprogrammed. User cannot configure the system to record specific events. All the events are that are recorded in the OpenLab ECM audit trail is preprogrammed. User cannot configure the system to record specific events in OpenLab ECM
Part 11 11.10(e)	4.9 Is previously recorded information left unchanged when records are changed?	S		Yes	OpenLab EZChrom with OpenLab ECM has the ability to store the changes as a new revision/ version and original records are left unchanged. OpenLab ECM has the ability to store the changes as a new revision /version and original records are left unchanged. During selection of results for further processing or reporting, the version of the result used can be chosen by the user.
Part 11 11.10(e)	4.10 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?	S, U		Yes	In OpenLab EZChrom audit trail information is securely stored and cannot be deleted by any user. Audit trail and associated metadata cannot be deleted as long as the associated file is stored in OpenLab ECM, as long as the defined record retention period has not expired.
Part 11 11.10(e)	4.11 Is audit trail available for review and copying by the FDA?	S		Yes	In OpenLab EZChrom audit trails can be viewed and exported for FDA review.
Annex 11	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?)	S	Annex 11, 8.1	Yes	In OpenLab EZChrom audit trails and result set can be reviewed, exported and printed. In OpenLab EZChrom and OpenLab ECM audit trails can be viewed and exported for FDA review.

5. Operational and Device Checks

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(f)	5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required?	S		Yes	The System does not enforce operational system check, however the system supports the following workflow which require the below sequence of steps to complete the workflow. – Acquire the measurement – Identify the peaks – Determine the peak area – Determine the amount of each material present using calibration – Customized calculation stored as part of the record – Create reports
Part 11 11.10(g)	5.2 Are there authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand?	S	Part 211, 68 b	Yes	Through user name, passwords and permissions OpenLab EZChrom supports configurable user roles that control system access at a detailed level. Access can be segregated and defined such that certain users have certain specific types of access to certain specific types of data sets while having different access to other types of data sets
	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S	Annex 11, 12.4	Yes	OpenLab EZChrom has the ability to record the user specific action with date and time stamps in audit trail and activity logs for every action perform within the system by the users. Operating system date and time are tracked through operating system logs.
Part 11 11.10(h)	5.4 Does the system allow to use device checks to determine, as appropriate, the validity of the source of data input or operational instruction?	S	There are two equally valid interpretations of this requirement. Systems should be designed such that: Proper communication is confirmed between the computer and the “source” of data input (i.e., the instrument) prior to transmission of instructions to or data from the “source.” Regulated records created by the system must unambiguously indicate the “source” of the data (i.e., which instrument or component generated the data.)	Yes	OpenLab EZChrom is designed to continually ensure a valid connection between the instrument and the computer workstation. OpenLab EZChrom has the ability to configure following system/instrument checks through the application to determine that the system is suitable for data acquisition and analysis, however it’s the user organization responsibility to enforce these checks within the system. – System suitability check: ▯ Noise ▯ drift ▯ ASTM noise short (unscaled) ▯ ASTM noise short (scaled) ▯ ASTM noise long (scaled) ▯ 6-sigma noise. – Baseline check: ▯ Drift ▯ Noise – Calibration – EMF (Early maintenance feedback)

5. Operational and Device Checks *continued*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.10(i)	5.5 Is there documented evidence that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	U	China GMP 18 Brazil 571	N/A	It is the responsibility of the user organization to maintain documented evidence that the persons who develop, maintain, or use electronic record and electronic signature systems have the education, training, and experience needed to perform these tasks Agilent software professionals involved in development of OpenLab CDS have received training in relevant aspects of data integrity.
Part 11 11.10(j)	5.6 Is there a written policy that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification?	U		N/A	It is the responsibility of the user organization to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
	5.7 Have employees been trained on this procedure?	U	Implied requirement of Part 11 11.10(j)	N/A	It is the responsibility of the user organization to train their staff.
Part 11 11.10(k)	5.8 Are there appropriate controls over systems documentation including:(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	U	China GMP 161 第五章系统 第十一条应当有详细阐述系统的文件（_必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序相接。	N/A	It is the responsibility of the user organization to establish systems documentation.
Part 11 11.10(i)	5.9 Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation?	S, U	第五章系统 第十七条计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。主要变更 应当经过验证。	Yes	Agilent maintains development and testing documentation for OpenLab EZChrom. Upon request, this documentation will be available to the user organization. It's the user organization responsibility to configure and validate the system per the intended use. It's the user organization responsibility to document the validation and configuration efforts through version control documents (specification, protocol, traceability matrix, summary reports, etc.)

6. Data Integrity, Date and Time Accuracy

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Annex 11	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?	S	Annex 11.5	Yes	Yes, OpenLab EZChrom has the ability to data export which could be used to exchange information with other systems. However, the validity of the data is user responsibility and the user responsibility is making sure that the export location is secured.
Annex 11	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.)	S,U	Annex 11-6 Brazil GMP 580 ICHQ7-5.45 第五章系统 第十五条当人工输入关键数据时(例如在称重过程中输入物料的重量和批号）_，应当复核输入记录以确保其准确性。这个复核可以由另外一个操作人员完成，或采用经验证的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。	Yes	Validity of the data entry in an electronic or manual form is the user's responsibility supported by SOP. For Data processing, review and approval is supported through electronic signature feature.
Clinical Computer Guide	6.3 Are controls established to ensure that the system's date and time are correct?	S, U	Clinical Computer Guide D.3	Yes	Agilent recommends that the system be configured to reference a timeserver to ensure accuracy of the system date and time. This is configured in and controlled by the operating system.
Clinical Computer Guide	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?	S	Clinical Computer Guide D.3	No	OpenLab EZChrom has the ability to limit the modification of the date and time stamps Note: This is usually limited to the System Administrator. This is configured and controlled by the operating system.
Clinical Computer Guide l	6.5 Are time stamps with a clear understanding of the time zone reference used implemented for systems that span different time zones?	S, U	Clinical Computer Guide D.3	Yes	Time stamps are shown in local time format for GMT format with offset to GMT time zone.

7. Control for Open Systems (Only applicable for open systems)

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.30	7.1 Are there procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt?	S, U		N/A	OpenLab EZChrom is not intended to be deployed as "open" system as per 21 CFR Part 11.3(b) (9).
Part 11 11.30	7.2 Are there additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality?	S		N/A	OpenLab EZChrom is not intended to be deployed as "open" system as per 21 CFR Part 11.3(b) (9).

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Annex 11	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?	S, U	Annex 11.14 ICH Q7.6.18 第五章系统 第二十三条电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。	Yes	Electronic signatures in OpenLab EZChrom are permanently linked to their respective records, which can be include in the final report. Signed electronic records show the name of the signer, and date and time the signature was executed, and the reason/meaning of the signature. It is user organizations responsibility to establish the legal impact of electronic signatures.
Part 11 11.50 (a)	8.2 Do signed electronic records contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer? (2) The date and time when the signature was executed? and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	S		Yes	The signed electronic records in OpenLab EZChrom show the name of the signer, and date and time the signature was executed, and the reason/meaning of the signature.
Part 11 11.50 (b)	8.3 Are the items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section subject to the same controls as for electronic records and are they included as part of any human readable form of the electronic record (such as electronic display or printout)?	S		Yes	In OpenLab EZChrom all electronic signature components are displayed and printed.
Part 11 11.70	8.4 Are electronic signatures and handwritten signatures linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	S		Yes	In OpenLab EZChrom electronic signatures are embedded in the result.
Part 11 Preamble	8.5 Is there a user specific automatic inactivity disconnect measure that would "de-log" the user if no entries or actions were taken within a fixed short timeframe?	S	Part 11 Preamble section 124	Yes	In OpenLab EZChrom automatic session locking enables the user organization to configure a time after which the user is automatically logged-out.

8. Electronic Signatures – Signature Manifestation and Signature/Record Linking *continued*

9. Electronic Signatures General Requirements and Signature Components and Controls

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	S, U		Yes	In OpenLab EZChrom each user has a unique login and thus a unique signature that cannot be used by another user.
Part 11 11.100(b)	9.2 Does the organization verify the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	S, U		N/A	It is the responsibility of the user organization to verify the identity of the user before they assign, certify an individual's electronic signature.
Part 11 11.100 (c)	9.3 Are persons using electronic signatures, prior to or at the time of such use, certified to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures? 9.4 Do persons using electronic signatures, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	U		N/A	It is the responsibility of the user organization to verify the identity of the user before they assign, certify an individual's electronic signature.
Part 11 11.200(a) (1)	9.5 Do electronic signatures that are not based upon biometrics employ at least two distinct identification components such as an identification code and password?	S, U		Yes	In OpenLab EZChrom both identification (user ID) and password are required to make an electronic signature.
Part 11 11.200(a) (1) (i)	9.6 When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components?	S		No	OpenLab EZChrom does not have the ability to executes a series of signature during a single, continuous period of controlled system access, however user can sign multiple record with the combination of user ID and password during a single controlled system access.
Part 11 11.200(a) (1) (i)	9.7 When an individual executes a series of signings during a single, continuous period of controlled system access, are subsequent signings executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?	S		Yes	OpenLab EZChrom does not have the ability executes a series of signature during a single, continuous period of controlled system access, however user can sign multiple record with the combination of user ID and password during a single controlled system access.
Part 11 11.200(a) (1) (ii)	9.8 When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	S		Yes	OpenLab EZChrom has the ability to enforce electronic signature by using user ID and password to make the signature unique.
Part 11 11.200(a) (2)	9.9 Are controls in place to ensure that electronic signatures that are not based upon biometrics are used only by their genuine owners?	S		Yes	OpenLab EZChrom has the ability to enforce electronic signature by using user ID and password to make the signature unique, however It is the responsibility of the user organization to verify the identity of the user before they assign, certify an individual's electronic signature.

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

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.200(a) (3)	9.10 Are the electronic signatures be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals?	S, U		Yes	In OpenLab EZChrom the user authentication is assign by the System Admin. Misuse of electronic signatures by anyone other than the owner would require intentional co-operation of a user and the System Administrator.
Part 11 11.200(b)	9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	S		No	OpenLab EZChrom does not support Biometric authentication.

10. Controls for Identification Codes and Passwords

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.300(a)	10.1 Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	S, U		Yes	OpenLab EZChrom does not allow duplicate user IDs.
Part 11 11.300(b)	10.2 Are controls in place to ensure that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	S, U		Yes	In OpenLab EZChrom password expiration is configurable in both local-account-based systems and Windows-Domain-security-based systems. The user organization should configure password expiration based on a documented risk assessment.
Part 11 11.300(c)	10.3 Are there procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromise tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	It is the responsibility of the user organization to establish these procedures.
Part 11 11.300(d)	10.4 Are there transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	It is the responsibility of the user organization to establish these transaction safeguards.

10. Controls for Identification Codes and Passwords *continued*

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Part 11 11.300(e)	10.5 Are there controls for initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	U		N/A	It is the responsibility of the user organization to establish controls to test devices initially as well as periodically to ensure they function properly and have not been altered in an unauthorized manner.

11. System Development and Support

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Annex 11	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	S, U	Annex 11 4.5 Brazil GMP 577 GAMP Comment: This is an example for a joint activity between user and supplier. The User should require from the supplier documented evidence that SW is developed in a QM System. The supplier has to develop the SW in a QMS 第二章原则 企业应当能够提供与供应商质量体系和审计信息相关的文件。	Yes	OpenLab EZChrom is developed within the ISO 9001 Quality Management per Agilent Product Life Cycle standards.

Part 11 Others	Requirements	S, U	Other regulations or comments	Yes/no	If yes, how, specifically, is the requirement satisfied using OpenLab EZChrom with OpenLab ECM? If no, what is the recommendation?
Brazil	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?	S, U	Brazil GMP 589 Again, joint activity. Supplier has must have such an agreement with subcontractor, the user must verify that the agreement is there. 第二章原则 第四条企业应当注重计算机化系统供应商的管理，制定相应的操作规程。供应商提供产品或服务时（如安装、配 置、集成、验证、维护、数据处理等），_企业应当与供应商签订正式协议，明确双方责任。	Yes	Agilent requires formal agreements with all suppliers and follows ISO 9001 Supplier Management policy.
ICH Q10	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	S, U	ICHQ10, 2.7 c	Yes	Agilent requires formal agreements with all suppliers and follows ISO 9001 Supplier Management policy.
ICH Q10	11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined?	S, U	ICHQ10, 2.7 c	Yes	Agilent requires formal agreements with all parties involved and follows ISO 9001 Supplier Management policy.
Part 11 11.10(i)	11.5 Is personnel developing and supporting software trained?	S, U	Again, joint activity, supplier must have people trained, user should have assurance, e.g., through audit that SW developers are trained, and training is documented, 第三章人员 第五条计算机化系统的"生命周期"中所涉及的各种活动，如验证、维护、管理等，需要各相关的职能部门人员之间的紧密合作。在职责中涉及使用和管理计算机化系统的人员，应当接受相应的使用和管理培训。确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训和指导。	Yes	All Agilent personnel are required to be trained (Ref. section 6.0 of the LSCA Quality Manual posted at Agilent.com/quality).

References

1. R. A. Botha and J. H. P Eloff. Separation of duties for access control enforcement in workflow environments. IBM Systems Journal – End-to-end security. 40 (3), 666-682. (2001).
2. U.S. Food and Drug Administration. CFR - Code of Federal Regulations Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A—General. Part 11 Electronic Records; Electronics Signatures [Online] **https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11** (accessed November 4, 2015).
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union. Volume 4. Good Manufacturing Practice. Medicinal Products for Human and Vetrinary Use. Annex 11. Computerised Systems. [Online] **http://ec.europa.eu/health/files/eudralex/**

vol-4/annex11_01-2011_en.pdf
(accessed November 4, 2015).

www.agilent.com/chem/OpenLab

Printed in the USA, July 15, 2019
5994-4685EN

Agilent
Trusted Answers