[ WHITE PAPER ]

Waters
THE SCIENCE OF WHAT'S POSSIBLE.™

# The Role of Empower Chromatography Data System in Assisting with Electronic Records Regulation Compliance

## INTRODUCTION

The objective of this white paper is to discuss the 21 CFR Part 11[1] and EU EudraLex Annex 11[2] compliance readiness of Waters™ Empower™ Software for the regulated scientific laboratory.

Regulated pharmaceutical and biotechnology companies serving the US market are currently striving to meet compliance with 21 CFR Part 11, the U.S. Food and Drug Administration's (FDA) rule governing electronic records and electronic signatures. Companies providing product for countries other than the USA, are also expected to meet the relevant electronic record and Data Integrity requirements from the governing Health Authorities of those countries, with the Medicines and Healthcare products Regulatory Agency (MHRA) taking a lead in this area. Additionally the World Health Organization (WHO) and the Pharmaceutical Inspection Cooperation Scheme (PIC/s) have issued guidances for managing electronic records and data.

Meeting Data Integrity expectations, including Part 11 compliance, remains challenging. However, e-record regulations will eventually be viewed as a significant driver to move companies from a paper-records environment to a more efficient and complete electronic-records environment. Although it is understood that merely purchasing a chromatography data software package that incorporates Part 11 or Annex 11 technical controls does not make a lab fully compliant or guarantee Data Integrity, technical controls should be inherent in any system used in a regulated environment. It is critical that these controls are understood, configured, validated, and utilized by the regulated company. A suite of technical controls for 21 CFR Part 11 and Annex 11 compliance are built into Empower to simplify administration and allow laboratories to meet global electronic record regulations.

## 21 CFR PART 11 BACKGROUND

Regulations affecting the creation, maintenance, transmission, storage, and modification of electronic records have added new focus to the regulated life science industries. 21 CFR Part 11 has emerged as one of the most defining regulations for the pharmaceutical and biotechnology industries along with the European counterpart, Good Manufacturing Practices (GMP) Annex 11. The impact is far-reaching, affecting quality assurance, quality control, information technology, manufacturing, and specifically lab management practices. 21 CFR Part 11, currently in force as part of all GxP inspections (i.e. Good Laboratory Practices (GLP) and Good Clinical Practices (GCP)) as well as GMP, has transformed the management of electronic data in regulated life science industries.

Every system that generates electronic records required by a predicate rule (GxP) must be examined to determine its current ability to comply with Part 11. Potentially, hundreds of systems within a pharmaceutical or biotechnology company may be affected. This includes analytical instruments (i.e., HPLC, UPLC,™ GC, MS, NMR, GC-MS, etc.), Microsoft® Excel® and Word documents, Laboratory Information Management Systems (LIMS), Electronic Laboratory Notebooks (ELNs), Scientific Data Management Systems (SDMS), and Laboratory Execution Systems (LES).

From the lab to the enterprise and beyond, Part 11 significantly impacts good electronic record management. The electronic records and signature rule, originally proposed by the pharmaceutical industry to reduce the burden of paper submissions in 1991, became effective in August 1997 for all companies wishing to sell food, pharmaceuticals, and cosmetics into the United States. Electronic record management and Data Integrity have recently gained momentum within FDA field operations as the enforcement of Part 11 has increased following extensive training of investigators and a significant distrust of non-contemporaneous paper reports.

## KNOW YOUR DATA

Machine-readable (raw) data and human-readable (report) data generated by analytical instruments (i.e., HPLC, UPLC, GC, UV, MS, etc.) and Microsoft Office tools are currently being maintained by a variety of inconsistent methods that make it difficult to either retrieve or reuse this data in an expeditious and uniform manner.

Raw data is defined as an electronic record the moment it is saved to durable media. Metadata (data about data) must also be saved and archived electronically. Since one cannot print to paper all metadata available in electronic form, and since the FDA wants to use the same tools to evaluate the data the operator used, paper printouts are no longer a suitable substitute for electronic data. Indeed, a Level 2 guidance[3] document was released on the www.fda.gov website (and included in the more recent DRAFT guidance on Data Integrity[4]), specifically indicating that paper copies of electronic records from complex systems such as chromatographs will not meet the GMP requirements. It is important that you maintain and protect the raw electronic data, the metadata and the report data for each regulated system. Electronic records should never be deleted even after summary reports have been printed.

Empower is designed to archive and catalog both the machine- and human-readable data, allowing companies to:

- Work in a way that is compliant to regulations on electronic records and electronic signatures.
- Meet global Data Integrity expectations.
- Archive machine-readable data from any controlled instrument to safe, stable and secure media.
- Retrieve previously archived machine-readable data as requested and within minutes.
- Establish traceability between the human-readable data and the machine-readable data.
- Integrate Empower with other applications to reduce transcription errors and additional human checking.

## SUMMARY OF WATERS STRATEGIES FOR COMPLIANCE

Empower uses Oracle® as the underlying relational database, providing a robust and scalable architecture. While Waters provides the sample application for Personal or Enterprise deployment, you can have more confidence in Data Integrity when deployed in an Enterprise Configuration.

Empower includes functionality which allows the regulated laboratory to simply configure and confidently demonstrate all of the technical requirements for global electronic record regulations, including 21 CFR Part 11, Annex 11 and other Data Integrity guidances. The current version of this product helps any regulated company meet the core requirements of Data Integrity with a clear plan and strategy for compliance, including the use of electronic signatures.

## SCOPE OF 21 CFR PART 11 (§11.1):

The general scope of Part 11 states:

*"The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."*

As the pharmaceutical and biotechnology industries move from paper to more flexible electronic data and information environments, Part 11 and other regulations will ensure continued Data Integrity in electronic formats. Overall, it is believed that more secure and trustworthy data results from Part 11 compliance in the life science arena.

In addition to enhancing the integrity of data required to be maintained by the predicate rules (the main regulations for research, development and manufacturing covered by the Federal Food, Drug, and Cosmetic Act or the Public Service Act) Part 11 also paves the way for full electronic submissions to the FDA through the electronic Common Technical Document gateway.

The Rule says: *"For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.... For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part."*

## ELECTRONIC RECORDS — APPLICABILITY AND DEFINITION

Per 21 CFR Part 11, the definition of an electronic record is: *"any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."*

21 CFR Part 11 applies to all electronic records used to meet GxP (GMP, GCP, GLP) requirements, including, but not limited to, systems for:

- Batch records, SOPs, test methods, specifications, and policies.
- Inventory records.
- Clinical and non-clinical study data.
- Calibration and preventative maintenance records.
- Validation protocols and reports.
- LIMS systems.
- Chromatography data systems.
- Customer-complaint files.
- Adverse event reporting systems.
- Automated document management systems.

Measures to ensure the trustworthiness of electronic records and electronic signatures consist of administrative, procedural, and technical controls implemented for computer systems.

To satisfy the entire requirement, regulated companies must employ oversight and review to monitor conformance of Data Integrity compliance. This discussion mainly focuses on the technical controls required by Part 11 that are provided by Empower for trustworthy and reliable scientific data management.

The following sections describe the key recommendations of Part 11 and how Empower aids in compliance to the described technical controls.

## CONTROLS FOR CLOSED SYSTEMS (§11.10):

Essentially, these are the measures designed to ensure the integrity of system operations and electronic records stored in a closed system.

Section 11.3 indicates that a *"Closed System means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."* By definition, Empower is a closed system.

The Rule further states that, *"Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."*

Some of the procedures and controls required to maintain record integrity in closed systems include:

- Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records (§11.10(a)).
- The ability to generate accurate and complete copies of records in both human-readable and electronic form suitable for inspection, review, and copying by the agency (§11.10(b)).
- Protection of records to enable accurate and ready retrieval throughout the records retention period (§11.10(c)).
- Limiting system access to authorized individuals (§11.10(d)).
- The use of computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation will be retained for a period as least as long as that required for the subject electronic records and will be available for agency review and copying (§11.10(e)).
- Use of operational system checks to enforce permitted sequencing of steps and events (§11.10(f)).
- Use of 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 (§11.10(g)).
- Use of device checks to determine the validity of the source of data input or operational instruction (§11.10(h)).

Let's take a look at some of the Part 11 technical controls in more detail.

## ACCURATE AND COMPLETE COPIES

§11.10(b) of the Rule states that one must have the ability to generate accurate and complete copies of records.

The ability to make accurate and complete copies of data and metadata in both human and electronic forms is very important.

***Human Readable Copies*** These might be for review purposes, for evidence in inspections, or for long-term archival. However the intended use of these copies needs to be clearly defined and is critical given that the FDA considers paper printouts of electronic records not suitable substitutes for those electronic records. The Level 2 guidance indicates the FDA recognize that for simple data, such as weight printout from a balance, a printed copy might be complete, but this is unlikely for complex instrument data, such as chromatography data systems. This exact same sentiment can be found in the MHRA GXP Data Integrity Definitions and Guidance, March 2018*.[5]

***Electronic Copies*** Archiving implies that data is moved from active state to inactive state and then may be moved and stored long term in a new location. Upon archiving, records must be protected to ensure record access and usability for the duration of the established record retention period. Controls must be implemented to ensure that archiving preserves the trusted status of the record and allows for long-term access and use.

Secure archiving requires:

- Moving data to a secure storage area that is readily retrievable.
- Maintaining the integrity of the data during a move.
- Validating the data move.
- Maintaining Data Integrity for the duration as defined in applicable record retention policies.
- Technology that preserves integrity of the record before, during, and after a data migration activity.
- Ensuring that the audit trail and any other metadata is archived along with instrument records.
- Technology and procedures that permit data to be retrieved and copied, in both electronic and human readable form, throughout the life of the data.

## PROTECTION AND READY RETRIEVAL OF RECORDS

§11.10(c) of the Rule states that records must be protected to enable their accurate and ready retrieval throughout the records retention period. Records should be protected against the likes of uncontrolled modification or deletion, and the system should automatically recognize when records have been altered after the initial recording.

The system must also allow for accurate and ready retrieval of such records. Part 11 does not specify a timeframe for the retention period; retention time is defined by the predicate rules.

The FDA's intention is that you should be able to generate your original results from your original raw data. To do that, you not only need the raw data but also the metadata, including methods and audit trails.

Data Integrity principles depend highly on protecting the original ('O' of the principles of ALCOA+) electronic data (i.e. not relying simply on paper or PDFs of reports, ensuring that data is both Enduring and Available (from the + principles of ALCOA+) throughout the lifecycle of the data.

Since Empower uses a relational database, it provides superior traceability of raw data to results, calibration curves, instrument methods, processing methods, and sample sets. In addition, Empower allows for immediate, but controlled, access to electronic data stored in its secure Oracle database.

- Capture both human-readable and machine-readable data accurately, electronically and automatically.
- Designed to retain records for as long as the designated retention period states.
- Dramatically reduce the amount of time required to properly manage the vast amount of data generated in labs every day.
- Work with complete confidence that the data is being safely and securely backed up and easily accessed when required.
- Automate archiving of complete projects/datasets to remove the need for manual archive of individual records.
- Archive entire groups of projects with a single click, or use additional automatic archiving tools such as those offered in Waters NuGenesis Laboratory Management System (LMS).

** It is not expected that these copies of data be viewable in any application other than the original software, or an updated version of the same application. Laboratory applications may be able to create exported or converted data for import into other applications, but these versions are unlikely to retain the entire metadata, meaning, or secure fidelity of truly archived data.*

## SERVER-BASED ENTERPRISE SOLUTIONS

The architecture of Empower Software is based on an Oracle database with distributed components to support enterprise-wide deployment. In an Enterprise deployment data is stored in a secure central server, normally located in a server room and not on vulnerable PCs or devices in the laboratory. Access to the data location is secured by the server operating system and regular users have no access to the raw data.

Empower provides buffering capabilities to protect data acquisition during server or network inaccessibility. Acquisition will continue according to the submitted sample set but data cannot be accessed, processed or evaluated until it is automatically uploaded to the secure database, once connection is re-established. Additionally, new sample sets cannot be submitted while in buffering mode.

Your Waters representative and network experts will help to design an acceptable level of hardware redundancy into your server configuration to protect against unexpected hardware failures, with minimum downtime.

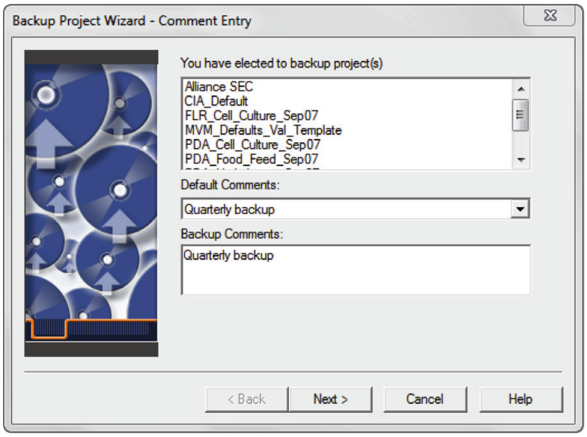
## AUTOMATED BACK UP OF “LIVE” GxP RECORDS USING AUTOMATED PROCESSES

As all data is in one location, automated procedures can be written and executed to provide electronic backups of the entire content of the Empower database and the associated files. A combination of cold backups, hot backups, and auto archive log files can restore an Empower Enterprise system to the exact point of failure, should there be any serious hardware errors.

## BACKUP OF COMPLETED LABORATORY DATA

It is imperative to capture the corresponding metadata along with the electronic record. Empower automatically creates electronic copies of all the metadata from both raw data and processed results in a project, preserving all traceability between results, methods, and audit trails, and stores this with the files, should you be required to remove it from your production Empower Enterprise environment.

- Empower backup software manages the project backup process and provides a mechanism to backup and archive several projects at one time (see Figure 1).
- It also gives you the option to have your own backup software started automatically when Empower is finished securing the project data (see Figure 2).
- You can easily retrieve backed-up data by using the restore function, which allows you to restore one or multiple projects (see Figure 3).



Backup Project Wizard - Comment Entry

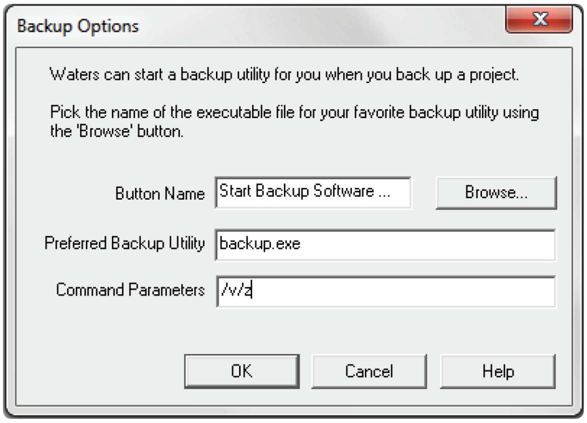
You have elected to backup project(s)

Alliance SEC
CIA_Default
FLR_Cell_Culture_Sep07
MVM_Defaults_Val_Template
PDA_Cell_Culture_Sep07
PDA_Food_Feed_Sep07

Default Comments: Quarterly backup

Backup Comments: Quarterly backup

*Figure 1. Project backup of multiple projects in one action in Empower.*



Backup Options

Waters can start a backup utility for you when you back up a project.

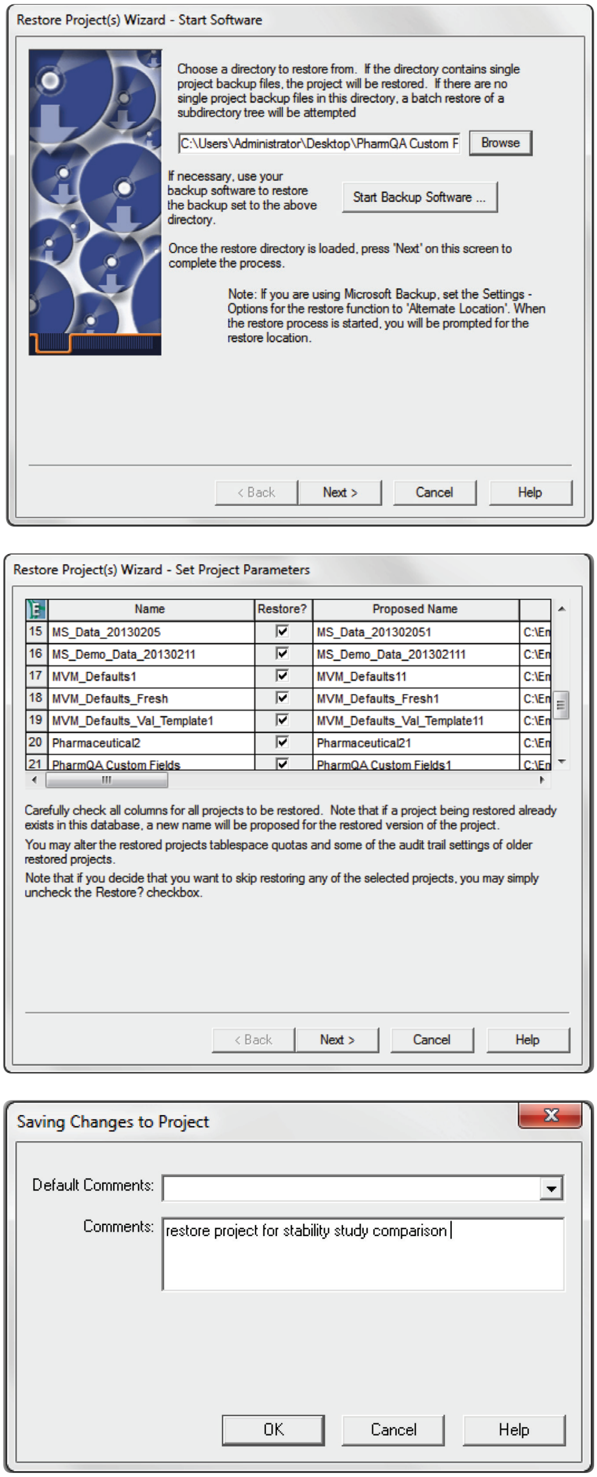
Pick the name of the executable file for your favorite backup utility using the 'Browse' button.

Button Name: Start Backup Software ...

Preferred Backup Utility: backup.exe

Command Parameters: /v/z

*Figure 2. How to configure preferred backup software in Empower.*



Restore Project(s) Wizard - Start Software

Choose a directory to restore from. If the directory contains single project backup files, the project will be restored. If there are no single project backup files in this directory, a batch restore of a subdirectory tree will be attempted

C:\Users\Administrator\Desktop\PharmQA Custom F

If necessary, use your backup software to restore the backup set to the above directory.

Once the restore directory is loaded, press 'Next' on this screen to complete the process.

Note: If you are using Microsoft Backup, set the Settings - Options for the restore function to 'Alternate Location'. When the restore process is started, you will be prompted for the restore location.

Restore Project(s) Wizard - Set Project Parameters

| E | Name | Restore? | Proposed Name | |
|---|---|---|---|---|
| 15 | MS_Data_20130205 | ☑ | MS_Data_201302051 | C:\En |
| 16 | MS_Demo_Data_20130211 | ☑ | MS_Demo_Data_201302111 | C:\En |
| 17 | MVM_Defaults1 | ☑ | MVM_Defaults11 | C:\En |
| 18 | MVM_Defaults_Fresh | ☑ | MVM_Defaults_Fresh1 | C:\En |
| 19 | MVM_Defaults_Val_Template1 | ☑ | MVM_Defaults_Val_Template11 | C:\En |
| 20 | Pharmaceutical2 | ☑ | Pharmaceutical21 | C:\En |
| 21 | PharmQA Custom Fields | ☑ | PharmQA Custom Fields1 | C:\En |

Carefully check all columns for all projects to be restored. Note that if a project being restored already exists in this database, a new name will be proposed for the restored version of the project.

You may alter the restored projects tablespace quotas and some of the audit trail settings of older restored projects.

Note that if you decide that you want to skip restoring any of the selected projects, you may simply uncheck the Restore? checkbox.

Saving Changes to Project

Default Comments:

Comments: restore project for stability study comparison

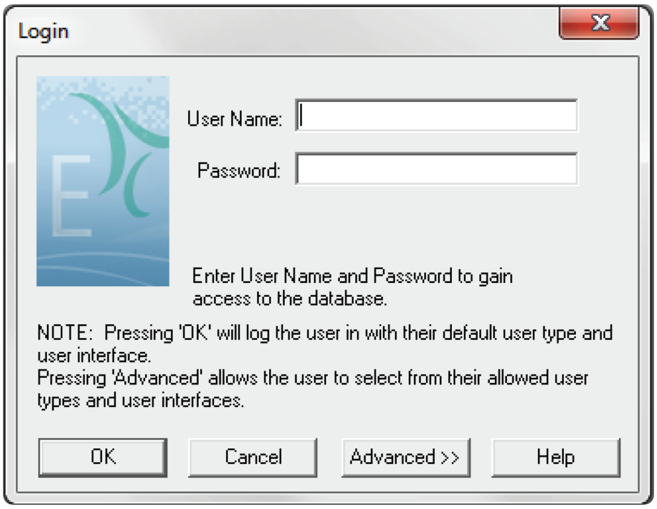
*Figure 3. The restore function of Empower. Restore has the ability to restore archived files either to their original location or to a new, user-specified location.*

## LIMITING SYSTEM ACCESS

Empower provides the ability to achieve compliance with §11.10(d) and §11.10(g) of the Electronics Records Rule as they describe control over access to the system, both limiting access to authorized users, and controlling the level of access to specific functions. Very similar access requirements exist in all e-record regulations and provide a key technical control to achieve the first ALCOA principle “Attributable”.

All Empower components are compliance-ready with these sub-sections provided the relevant access and system polices have been configured, and suitable procedural and administrative controls are also in place.

- Empower requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data.
- Empower includes a defined workflow (instrument set up, data collection, integration, calibration/quantitation, and reporting) ensuring that proper sequencing of steps and events are followed. These steps (including any rework processes) should be documented in Standard Operating Procedures (SOPs).



Login

User Name:

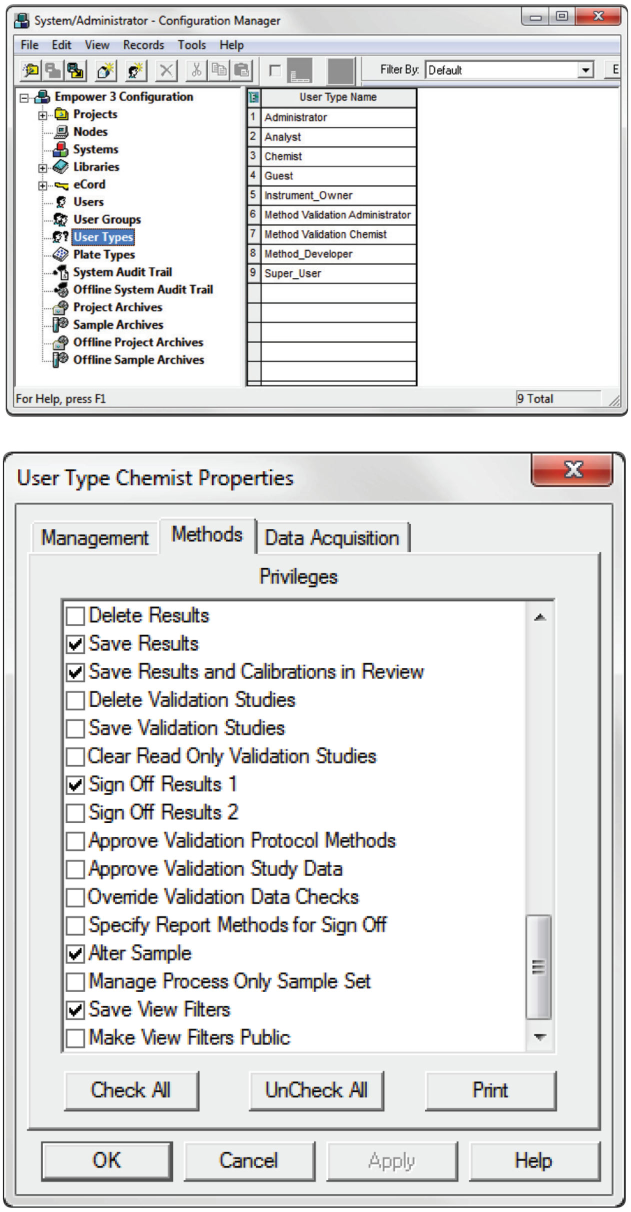
Password:

Enter User Name and Password to gain access to the database.

NOTE: Pressing 'OK' will log the user in with their default user type and user interface.
Pressing 'Advanced' allows the user to select from their allowed user types and user interfaces.

*Figure 4. Empower login screen. This system uses a login that requires the user to enter both the username and password, helping to protect access to the records therein.*

- For enhanced records protection and access control, Empower assigns detailed privileges to users and user groups (i.e., not just read/write/delete access). For example, someone with pre-defined Chemist privileges would only be allowed to sign reports for review, without the capability of approving them.



| | User Type Name |
|---|---|
| 1 | Administrator |
| 2 | Analyst |
| 3 | Chemist |
| 4 | Guest |
| 5 | Instrument_Owner |
| 6 | Method Validation Administrator |
| 7 | Method Validation Chemist |
| 8 | Method_Developer |
| 9 | Super_User |

- □ Delete Results
- ☑ Save Results
- ☑ Save Results and Calibrations in Review
- □ Delete Validation Studies
- □ Save Validation Studies
- □ Clear Read Only Validation Studies
- ☑ Sign Off Results 1
- □ Sign Off Results 2
- □ Approve Validation Protocol Methods
- □ Approve Validation Study Data
- □ Override Validation Data Checks
- □ Specify Report Methods for Sign Off
- ☑ Alter Sample
- □ Manage Process Only Sample Set
- ☑ Save View Filters
- □ Make View Filters Public

*Figure 5. Empower 3 chemist privileges. Defined user privileges such as the ability to sign-off results at Level 1 only.*

## DEVICE MANAGEMENT

11.10(h) describes “device checks” and uses the example of terminals as a point of entry of data. For CDS solutions it is more applicable to consider devices as chromatography instruments, which are the main source of data input.

Empower will capture data from any instrument or device that the user specifies. A valid instrument driver, and possibly a license, needs to be installed, and the specific instrument must be configured in the Empower application.

As well as directly controlled LC, GC, CE, and MS instruments, Empower can collect data from any device that will output an analog signal into a convertor called a SAT/IN. This data will be transferred to Empower and can be processed just as if it came from a directly controlled instrument.

Qualification of instruments and SAT/IN devices will help to show adherence to this section of the rule, as well as complying with other GMP and GLP regulations regarding calibration or checking of equipment.

## AUDIT TRAILS

The use of computer generated, time-stamped audit trails is a significant part of the “Controls for Closed Systems” (§11.10(e)). Audit trails form an essential component of any e-record compliance or data integrity toolset needed to meet  regulations and guidances from across the globe, covering GMP, GLP, and GCP data, as well as part of the identification of altered records as specified in 11.10(a), as well as regulations and guidances from across the globe, covering GMP, GLP, and GCP data.

An example of this is the April 2016 OECD Guidance Number 17 for Applications of GLP Principles to Computerized Systems[6]: “An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point.”

Audit trails are considered the key to the security of a system since they track changes to the data and metadata. In this way, an incomplete or absent audit trail can impact Data Integrity or even product quality. The absence of an audit trail is considered to be “highly significant when there are data discrepancies” according to the FDA.[7]

Part 11 requires electronic audit trails for all data archived and managed as per the Rule. Audit trails must be:

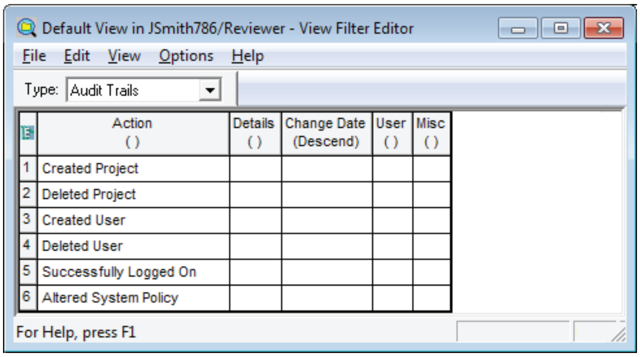
- Inclusive of the date and time when the individual created, modified, reviewed, approved or deleted an electronic record in an unambiguous format.
- Computer generated (automatically).
- Secure — adequate security to prevent tampering.
- Operator independent — no operator or administrator may change or modify in any way.

Change actions need to be documented in the audit trail and the recorded changes must not obscure previously recorded information (i.e., record the “before” and “after” values).

Additionally, users are required to record a scientific justification of "why" the changes have been made. This is normally documented in a comment or reason field.

The audit trail documentation must be retained for the same period as the electronic record. Accurate and complete copies must be made available to the FDA for review and copying and must be both human-readable and machine-readable.

- Empower System Audit Trail provides a history of actions that affects the overall system configuration (such as denied login, project archival, changes to system policies).
- The System Audit Trail tracks critical actions such as changes to users privileges.
- All audit trails are generated automatically, cannot be modified, and include all Administrator activity.

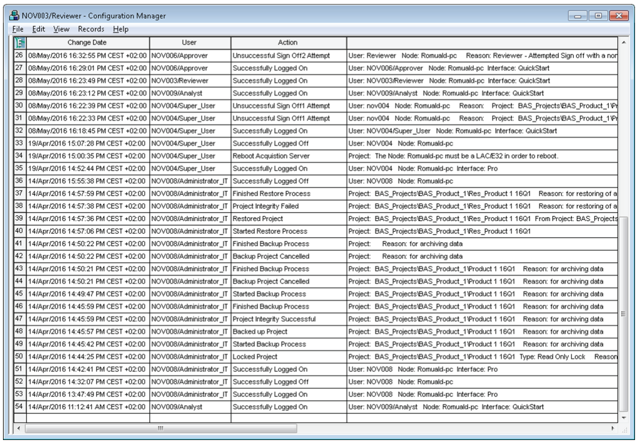


Default View in JSmith786/Reviewer - View Filter Editor

Type: Audit Trails

| | Action<br>( ) | Details<br>( ) | Change Date<br>(Descend) | User<br>( ) | Misc<br>( ) |
|---|---|---|---|---|---|
| 1 | Created Project | | | | |
| 2 | Deleted Project | | | | |
| 3 | Created User | | | | |
| 4 | Deleted User | | | | |
| 5 | Successfully Logged On | | | | |
| 6 | Altered System Policy | | | | |

For Help, press F1



NOV003/Reviewer - Configuration Manager

| | Change Date | User | Action | |
|---|---|---|---|---|
| 26 | 08/May/2016 16:32:55 PM CEST +02:00 | NOV006/Approver | Unsuccessful Sign Off2 Attempt | User: Reviewer Node: Romuald-pc Reason: Reviewer - Attempted Sign off with a nor |
| 27 | 08/May/2016 16:29:01 PM CEST +02:00 | NOV006/Approver | Successfully Logged On | User: NOV006/Approver Node: Romuald-pc Interface: QuickStart |
| 28 | 08/May/2016 16:23:49 PM CEST +02:00 | NOV003/Reviewer | Successfully Logged On | User: NOV003/Reviewer Node: Romuald-pc Interface: QuickStart |
| 29 | 08/May/2016 16:23:12 PM CEST +02:00 | NOV009/Analyst | Successfully Logged On | User: NOV009/Analyst Node: Romuald-pc Interface: QuickStart |
| 30 | 08/May/2016 16:22:39 PM CEST +02:00 | NOV004/Super_User | Unsuccessful Sign Off1 Attempt | User: nov004 Node: Romuald-pc Reason: Project: BAS_Projects\BAS_Product_1\Pr |
| 31 | 08/May/2016 16:22:33 PM CEST +02:00 | NOV004/Super_User | Unsuccessful Sign Off1 Attempt | User: nov004 Node: Romuald-pc Reason: Project: BAS_Projects\BAS_Product_1\Pr |
| 32 | 08/May/2016 16:18:45 PM CEST +02:00 | NOV004/Super_User | Successfully Logged On | User: NOV004/Super_User Node: Romuald-pc Interface: QuickStart |
| 33 | 19/Apr/2016 15:07:28 PM CEST +02:00 | NOV004/Super_User | Successfully Logged Off | User: NOV004 Node: Romuald-pc |
| 34 | 19/Apr/2016 15:00:35 PM CEST +02:00 | NOV004/Super_User | Reboot Acquistion Server | Project: The Node: Romuald-pc must be a LAC/E32 in order to reboot. |
| 35 | 19/Apr/2016 14:52:44 PM CEST +02:00 | NOV004/Super_User | Successfully Logged On | User: NOV004 Node: Romuald-pc Interface: Pro |
| 36 | 14/Apr/2016 15:55:38 PM CEST +02:00 | NOV008/Administrator_IT | Successfully Logged Off | User: NOV008 Node: Romuald-pc |
| 37 | 14/Apr/2016 14:57:59 PM CEST +02:00 | NOV008/Administrator_IT | Finished Restore Process | Project: BAS_Projects\BAS_Product_1\Res_Product 1 16Q1 Reason: for restoring of a |
| 38 | 14/Apr/2016 14:57:38 PM CEST +02:00 | NOV008/Administrator_IT | Project Integrity Failed | Project: BAS_Projects\BAS_Product_1\Res_Product 1 16Q1 Reason: for restoring of a |
| 39 | 14/Apr/2016 14:57:36 PM CEST +02:00 | NOV008/Administrator_IT | Restored Project | Project: BAS_Projects\BAS_Product_1\Res_Product 1 16Q1 From Project: BAS_Projects |
| 40 | 14/Apr/2016 14:57:06 PM CEST +02:00 | NOV008/Administrator_IT | Started Restore Process | Project: BAS_Projects\BAS_Product_1\Res_Product 1 16Q1 |
| 41 | 14/Apr/2016 14:50:22 PM CEST +02:00 | NOV008/Administrator_IT | Finished Backup Process | Project: Reason: for archiving data |
| 42 | 14/Apr/2016 14:50:22 PM CEST +02:00 | NOV008/Administrator_IT | Backup Project Cancelled | Project: Reason: for archiving data |
| 43 | 14/Apr/2016 14:50:21 PM CEST +02:00 | NOV008/Administrator_IT | Finished Backup Process | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 44 | 14/Apr/2016 14:50:21 PM CEST +02:00 | NOV008/Administrator_IT | Backup Project Cancelled | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 45 | 14/Apr/2016 14:49:47 PM CEST +02:00 | NOV008/Administrator_IT | Started Backup Process | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 46 | 14/Apr/2016 14:45:59 PM CEST +02:00 | NOV008/Administrator_IT | Finished Backup Process | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 47 | 14/Apr/2016 14:45:59 PM CEST +02:00 | NOV008/Administrator_IT | Project Integrity Successful | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 48 | 14/Apr/2016 14:45:57 PM CEST +02:00 | NOV008/Administrator_IT | Backed up Project | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 49 | 14/Apr/2016 14:45:42 PM CEST +02:00 | NOV008/Administrator_IT | Started Backup Process | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Reason: for archiving data |
| 50 | 14/Apr/2016 14:44:25 PM CEST +02:00 | NOV008/Administrator_IT | Locked Project | Project: BAS_Projects\BAS_Product_1\Product 1 16Q1 Type: Read Only Lock Reason |
| 51 | 14/Apr/2016 14:42:41 PM CEST +02:00 | NOV008/Administrator_IT | Successfully Logged On | User: NOV008 Node: Romuald-pc Interface: Pro |
| 52 | 14/Apr/2016 14:32:07 PM CEST +02:00 | NOV008/Administrator_IT | Successfully Logged Off | User: NOV008 Node: Romuald-pc |
| 53 | 14/Apr/2016 13:47:49 PM CEST +02:00 | NOV008/Administrator_IT | Successfully Logged On | User: NOV008 Node: Romuald-pc Interface: Pro |
| 54 | 14/Apr/2016 11:12:41 AM CEST +02:00 | NOV009/Analyst | Successfully Logged On | User: NOV009/Analyst Node: Romuald-pc Interface: QuickStart |

*Figure 6. The readable view of the Empower system audit trail which can be filtered and sorted to find and print relevant records.*

The Empower Project Audit Trail is an overview of every activity performed by users, as well as data, metadata, and methods inside the project. It captures information that affects the data within a project (calibration, method changes, processing data) and other information captured in the Empower database (who, when, what) including any data insertions, modifications to metadata, record copies, deletions, and applications of review or approval signatures.

Further details can be found in individual item histories such as Acquisition and Injection Logs, Method Audit Trails, Sample, or Sample Set Histories.

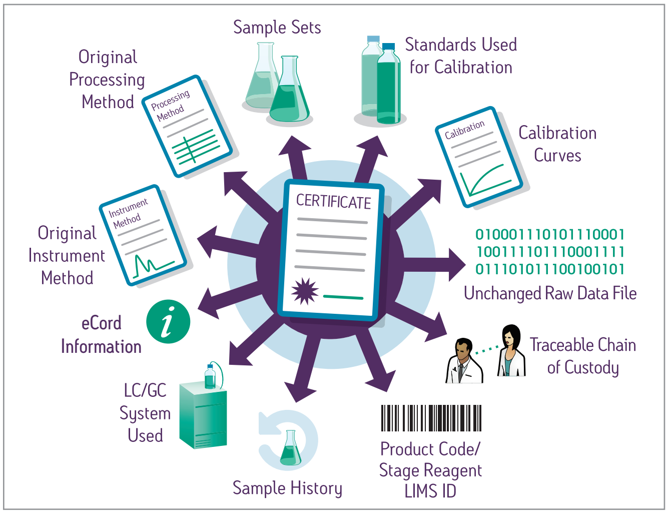


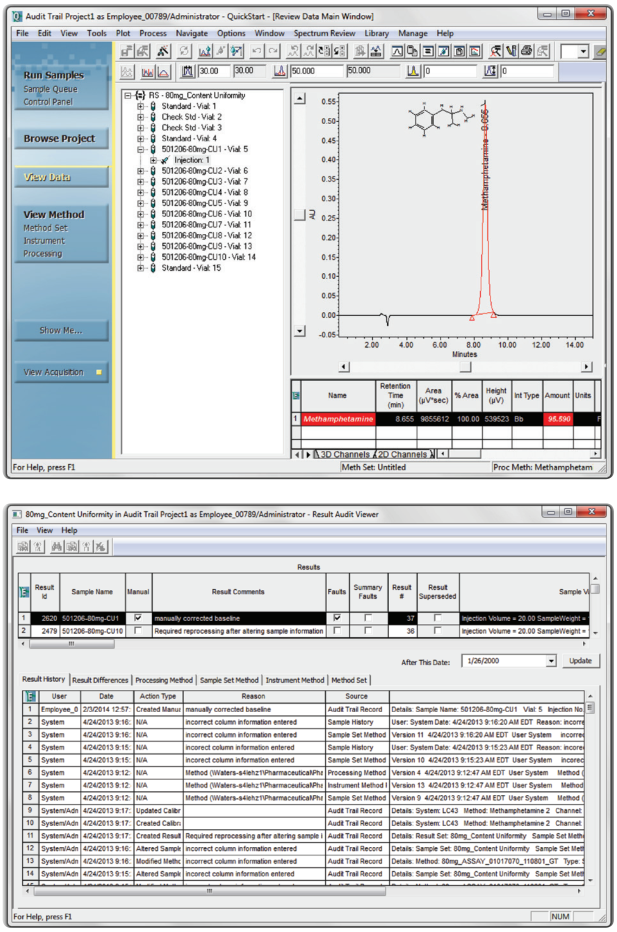
*Figure 7. The Oracle database underlying Empower creates permanent linking relations between methods, data, and metadata which cannot be broken, permitting easy review of related data.*

Additional capabilities of Empower:

- Ability to discern invalid or altered records using records in the project audit trail.
- Automatically create new and discrete records of changes made to methods and results, while preserving the original and allowing for comparison by highlighting the differences.
- Provide Checksum and Cyclic Redundancy Check (CRC) verification for all human-readable and machine-readable data to protect against data alterations through external access to the system.

New requirements of European regulations (GMP Annex 11) to regularly review audit trails are also being expected by FDA investigators. Even though there is no formal mention of this in Part 11, companies that fail to have a formal process to review audit trails have had this omission cited in official warning letters. Most laboratories treat audit trails relating directly to data and results as part of the metadata needing to be reviewed before batch or study release, while system level audit trails fall under a periodic review by administrators SOP.

Empower can assist in meeting this expectation by providing easy access to methods, data, results, and metadata audit trails from the review screen.



Audit Trail Project1 as Employee_00789/Administrator - QuickStart - [Review Data Main Window]

- RS - 80mg_Content Uniformity
  - Standard - Vial: 1
  - Check Std - Vial: 2
  - Check Std - Vial: 3
  - Standard - Vial: 4
  - 501206-80mg-CU1 - Vial: 5
    - Injection: 1
  - 501206-80mg-CU2 - Vial: 6
  - 501206-80mg-CU3 - Vial: 7
  - 501206-80mg-CU4 - Vial: 8
  - 501206-80mg-CU5 - Vial: 9
  - 501206-80mg-CU6 - Vial: 10
  - 501206-80mg-CU7 - Vial: 11
  - 501206-80mg-CU8 - Vial: 12
  - 501206-80mg-CU9 - Vial: 13
  - 501206-80mg-CU10 - Vial: 14
  - Standard - Vial: 15

| | Name | Retention Time (min) | Area (µV*sec) | % Area | Height (µV) | Int Type | Amount | Units |
|---|---|---|---|---|---|---|---|---|
| 1 | Methamphetamine | 8.655 | 9855612 | 100.00 | 539523 | Bb | 95.590 | F |

80mg_Content Uniformity in Audit Trail Project1 as Employee_00789/Administrator - Result Audit Viewer

Results

| | Result Id | Sample Name | Manual | Result Comments | Faults | Summary Faults | Result # | Result Superseded | Sample Vi |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2620 | 501206-80mg-CU1 | ☑ | manually corrected baseline | ☑ | □ | 37 | □ | Injection Volume = 20.00 SampleWeight = |
| 2 | 2479 | 501206-80mg-CU10 | □ | Required reprocessing after altering sample information | □ | □ | 36 | □ | Injection Volume = 20.00 SampleWeight = |

| | User | Date | Action Type | Reason | Source | |
|---|---|---|---|---|---|---|
| 1 | Employee_0 | 2/3/2014 12:57: | Created Manua | manually corrected baseline | Audit Trail Record | Details: Sample Name: 501206-80mg-CU1 Vial: 5 Injection No. |
| 2 | System | 4/24/2013 9:16: | N/A | incorrect column information entered | Sample History | User: System Date: 4/24/2013 9:16:20 AM EDT Reason: incorre |
| 3 | System | 4/24/2013 9:16: | N/A | incorrect column information entered | Sample Set Method | Version 11 4/24/2013 9:16:20 AM EDT User System incorre |
| 4 | System | 4/24/2013 9:15: | N/A | incorect column information entered | Sample History | User: System Date: 4/24/2013 9:15:23 AM EDT Reason: incore |
| 5 | System | 4/24/2013 9:15: | N/A | incorect column information entered | Sample Set Method | Version 10 4/24/2013 9:15:23 AM EDT User System incorec |
| 6 | System | 4/24/2013 9:12: | N/A | Method (\\Waters-s4lehz1\PharmaceuticalPha | Processing Method | Version 4 4/24/2013 9:12:47 AM EDT User System Method ( |
| 7 | System | 4/24/2013 9:12: | N/A | Method (\\Waters-s4lehz1\PharmaceuticalPha | Instrument Method I | Version 13 4/24/2013 9:12:47 AM EDT User System Method |
| 8 | System | 4/24/2013 9:12: | N/A | Method (\\Waters-s4lehz1\PharmaceuticalPha | Sample Set Method | Version 9 4/24/2013 9:12:47 AM EDT User System Method ( |
| 9 | System/Adn | 4/24/2013 9:17: | Updated Calibr | | Audit Trail Record | Details: System: LC43 Method: Methamphetamine 2 Channel: |
| 10 | System/Adn | 4/24/2013 9:17: | Created Calibr | | Audit Trail Record | Details: System: LC43 Method: Methamphetamine 2 Channel: |
| 11 | System/Adn | 4/24/2013 9:17: | Created Result | Required reprocessing after altering sample i | Audit Trail Record | Details: Result Set: 80mg_Content Uniformity Sample Set Meth |
| 12 | System/Adn | 4/24/2013 9:16: | Altered Sampl | incorrect column information entered | Audit Trail Record | Details: Sample Set: 80mg_Content Uniformity Sample Set Meth |
| 13 | System/Adn | 4/24/2013 9:16: | Modified Methc | incorrect column information entered | Audit Trail Record | Details: Method: 80mg_ASSAY_01017070_110801_GT Type: S |
| 14 | System/Adn | 4/24/2013 9:15: | Altered Sampl | incorect column information entered | Audit Trail Record | Details: Sample Set: 80mg_Content Uniformity Sample Set Meth |

*Figure 8. The Review window and the Result Audit Viewer facilitate a reviewer to interrogate the data, methods, peak results, calibration curves, and audit records, and then take the results directly to Preview to electronically sign off.*

A tool in Empower, called the Result Audit Viewer, brings together audit records from the acquisition log, project, method, and sample histories into a single window, and also permits easy comparison of methods and results.

Documentation of audit trail review should be performed in a similar way to documentation of any review process. Typically this is done by signing the results as 'reviewed' or 'approved', following a data review SOP which outlines how the review process should be performed, and will include how and when to review audit trails.

The WHO Guidance[8] notes under the section for documentation of data review on paper records, a signature should be added to the actual records reviewed, while, in the "expectations for electronic records" you follow a clear review procedure and then electronically sign the electronic data set as having been reviewed and approved. Separately documenting review of audit trails is not expected.

## CONTROLS FOR OPEN SYSTEMS (§11.30):

21 CFR Part 11 states: *"Open System means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."*

It is further stated that: *"Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ 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. Such procedures and controls shall include those identified in §11.10, as appropriate, and 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."*

An example of such an open system is an unsecured, web-based system used for transmitting data. Subpart B, §11.30 states that the controls for closed systems also apply to open systems. However, in order to maintain the authenticity, integrity, and confidentiality of electronic records that are transmitted over an open system, tighter controls such as digital encryption would be required. Empower is not considered an open system.

## ELECTRONIC SIGNATURES — APPLICABILITY AND DEFINITION

Part 11 defines an electronic signature as: *"a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature."*

Many companies are not ready for e-signatures, but must still comply with all of the regulations regarding electronic records. The FDA is permitting the use of a hybrid system for companies that maintain archives of the electronic versions of each record while concurrently using paper-based signature processes.

It is vital to be able to prove the identity of an individual required to sign an electronic record. The key is linking the owner to the electronic identity and confirming that the individual has the authority to sign.

## ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS (§11.200):

Electronic signatures may be either non-biometric or biometric. For non-biometric electronic signatures, two forms of identification are required. These can be any of the following:

- User ID and password.
- Card key and password.
- Two passwords.

*"§11.200(a) Electronic signatures that are not based upon biometrics shall:*

1. *Employ at least two distinct identification components such as an identification code and password.*
2. *Be used only by their genuine owners; and*
3. *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."*

The Rule defines Biometric as: *"A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable actions(s) where those features and/or actions are both unique to that individual and measurable."*

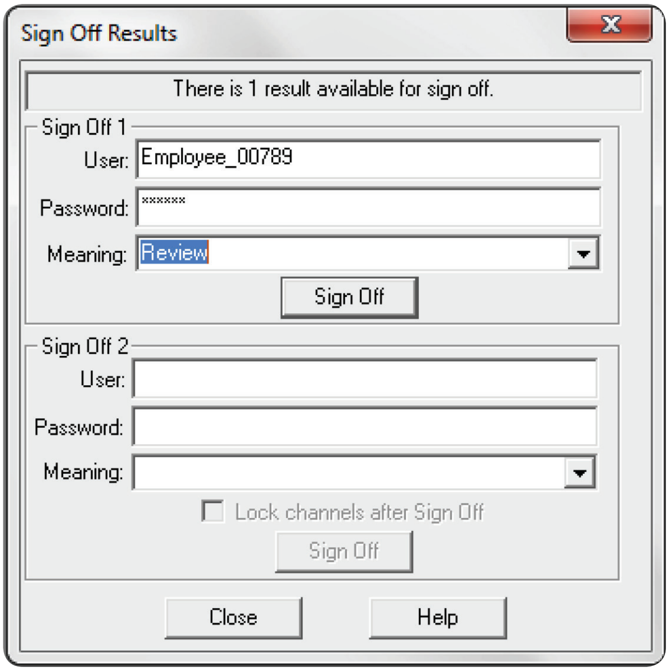
Some familiar examples include voiceprints, finger/thumb print recognition, retinal scans, or any device or method designed to ensure use only by the genuine owner.

- Empower does not provide biometric signature capabilities. However, third party tools to convert biometric readings to traditional username/password combination may be implemented.

Non-biometric e-signatures must be administered and executed to prevent forging.

Empower Software:

- Provides the ability to achieve compliance with this part of the rule.
- Requires a username/password combination in order to e-sign a result or a set of results.
- Ensures all pages of the report are reviewed before sign off is permitted.
- Allows permission-based controls around who can sign results at each level.
- Provides sign off policies to personalize your sign off practices.
- Result Sign Off Policies allow compliance with requirements for signatures that are either expressed in 21 CFR Part 11 or in predicate rules (GxP). Setting these only affects the use of electronic signatures in Empower.
- May be set to create and store a PDF of the actual report used for sign off. This PDF can be saved inside the Empower database or be set to save in Waters NuGenesis™ SDMS, if required.



Sign Off Results

There is 1 result available for sign off.

Sign Off 1

User: Employee_00789

Password: ******

Meaning: Review

Sign Off 2

User:

Password:

Meaning:

□ Lock channels after Sign Off

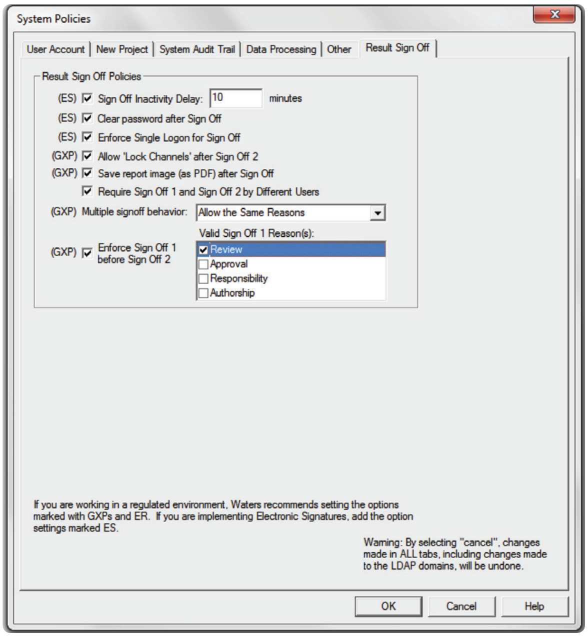
*Figure 9. Empower uses a combination of username and password to sign a result. A meaning is also required and, while two levels of sign off with different associated privileges are seen in the box, results can be signed multiple times at each level.*

The regulation has a series of rules about the use of one or both of the signature components in a contiguous session:

§11.200(a)(1) (ii) *"The first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual."*

ii) *"When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components."*

- Within Empower, each time you sign a report in a contiguous fashion, both the username and password are required for authentication for the first signature, but only a password is required for subsequent signings.
- Timeouts on the sign-off screen ensure that a new sign-off session is started if the system is left idle, ensuring that both parts of the signature are required when the session is resumed.



Result Sign Off Policies

(ES) ☑ Sign Off Inactivity Delay: 10 minutes
(ES) ☑ Clear password after Sign Off
(ES) ☑ Enforce Single Logon for Sign Off
(GXP) ☑ Allow 'Lock Channels' after Sign Off 2
(GXP) ☑ Save report image (as PDF) after Sign Off
☑ Require Sign Off 1 and Sign Off 2 by Different Users
(GXP) Multiple signoff behavior: Allow the Same Reasons
(GXP) ☑ Enforce Sign Off 1 before Sign Off 2

Valid Sign Off 1 Reason(s):
☑ Review
☐ Approval
☐ Responsibility
☐ Authorship

If you are working in a regulated environment, Waters recommends setting the options marked with GXPs and ER. If you are implementing Electronic Signatures, add the option settings marked ES.

Warning: By selecting "cancel", changes made in ALL tabs, including changes made to the LDAP domains, will be undone.

*Figure 10. Empower allows you to create a unique sign-off policy.*

## SIGNATURE MANIFESTATIONS (§11.50):

21 CFR Part 11 does not mandate electronic signatures, nor does it mandate when an e-signature is used or what documents must be signed. This is governed by the predicate rules and generally includes the signature of the author/creator of the data and the signature of the reviewer who approves the data. However, many companies will have their own SOPs about how records are reviewed and approved.

The US Regulation does, however, require e-signature manifestations to contain three key pieces of metadata.
It is stated that:
*"(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:*

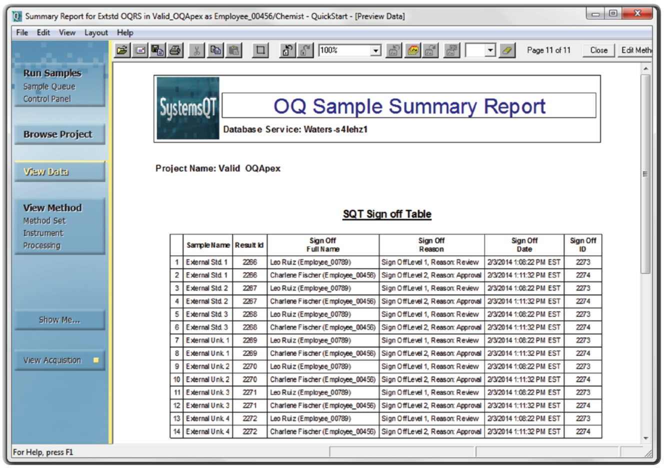
1. *The printed name of the signer;*
2. *The date and time when the signature was executed; and*
3. *The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*

*(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human-readable form of the electronic record (such as electronic display or printout)."*

- Empower provides the ability to achieve compliance with this part of the rule.
- The software captures and displays the three pieces of metadata of which a signature manifestation should consist.
- The Empower e-signature displays:
  - the full printed name of the signer,
  - the date and the time that the signature was executed, and
  - a meaning for the signature (configure defined meanings in the Configuration Manager for review, approval, authorship, responsibility, etc.).

For trustworthy signed electronic records, electronic signatures should be unique to one individual and should not be reused or reassigned to anyone else:

- Empower prevents re-allocation of e-signatures to another user and prevents deletion of a user/signer once it has been created.



OQ Sample Summary Report

Database Service: Waters-s4lehz1

Project Name: Valid OQApex

SQT Sign off Table

| | Sample Name | Result Id | Sign Off<br>Full Name | Sign Off<br>Reason | Sign Off<br>Date | Sign Off<br>ID |
|---|---|---|---|---|---|---|
| 1 | External Std. 1 | 2266 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 2 | External Std. 1 | 2266 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 3 | External Std. 2 | 2267 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 4 | External Std. 2 | 2267 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 5 | External Std. 3 | 2268 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 6 | External Std. 3 | 2268 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 7 | External Unk. 1 | 2269 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 8 | External Unk. 1 | 2269 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 9 | External Unk. 2 | 2270 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 10 | External Unk. 2 | 2270 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 11 | External Unk. 3 | 2271 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 12 | External Unk. 3 | 2271 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |
| 13 | External Unk. 4 | 2272 | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review | 2/3/2014 1:08:22 PM EST | 2273 |
| 14 | External Unk. 4 | 2272 | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval | 2/3/2014 1:11:32 PM EST | 2274 |

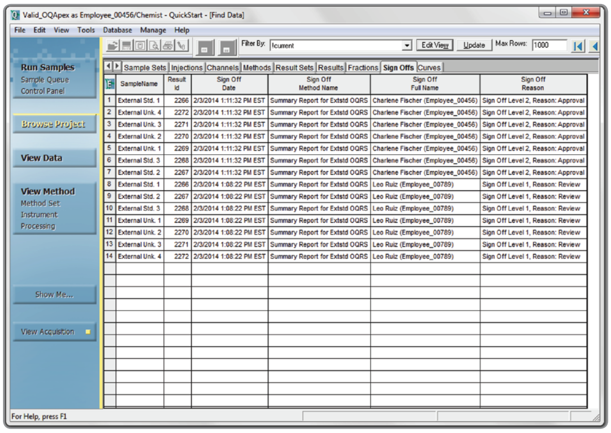
*Figure 11. An Empower display of e-signature history. Note the display in human-readable form of the three pieces of metadata needed for an e-signature manifestation.*

## SIGNATURE RECORD LINKING (§11.70):

Section 11.70 ensures the integrity of either electronic or handwritten signatures executed to electronic records by specifying that: *"Electronic signatures and handwritten signatures executed to electronic records shall be 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."*

Linking the signature to the original electronic record is especially critical when a printout or an electronic copy of the e-record becomes orphaned from that e-record. The signature must not be lost.

- Empower provides the ability to achieve compliance with this part of the rule.
- The software enables non-breakable linking of electronic signatures to electronic records.
- The Empower e-signature information is stored in the Oracle relational database and is permanently linked to the record itself.
- It is not possible to excise, copy, or transfer the signature to another unsigned document.



Filter By: !current

Max Rows: 1000

| | SampleName | Result Id | Sign Off Date | Sign Off Method Name | Sign Off Full Name | Sign Off Reason |
|---|---|---|---|---|---|---|
| 1 | External Std. 1 | 2266 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 2 | External Unk. 4 | 2272 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 3 | External Unk. 3 | 2271 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 4 | External Unk. 2 | 2270 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 5 | External Unk. 1 | 2269 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 6 | External Std. 3 | 2268 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 7 | External Std. 2 | 2267 | 2/3/2014 1:11:32 PM EST | Summary Report for Extstd OQRS | Charlene Fischer (Employee_00456) | Sign Off Level 2, Reason: Approval |
| 8 | External Std. 1 | 2266 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 9 | External Std. 2 | 2267 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 10 | External Std. 3 | 2268 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 11 | External Unk. 1 | 2269 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 12 | External Unk. 2 | 2270 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 13 | External Unk. 3 | 2271 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |
| 14 | External Unk. 4 | 2272 | 2/3/2014 1:08:22 PM EST | Summary Report for Extstd OQRS | Leo Ruiz (Employee_00789) | Sign Off Level 1, Reason: Review |

*Figure 12. The permanent Empower Signoffs Oracle table is updated after each signature event. This table can only be added to by the application (i.e., more signatures can be added to a result), but cannot be changed or altered.*

## CONTROLS FOR IDENTIFICATION CODES/ PASSWORDS (§11.300):

Ultimately, the purpose of Part 11, and other related record regulations, is to achieve trusted electronic records. The identity of the user is essential to irrefutably label an individual responsible for some aspect of the electronic record. In terms of Data Integrity this is known as the "Attributable" principle. Electronic identification is the passive harvesting of users' identities as they are performing tasks on a system.

Some characteristics of electronic identification include:

- Users typically assigned an ID as part of system. The ID is passively captured/harvested as the user operates the system.
- If an electronic ID is collected, it must be linked to the record for the duration of the record.
- Electronic ID does not have the same force of law as electronic signature; however, it still implies responsibility and should be taken seriously.

*§11.300 Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity.*

*Such controls shall include:*

*a. Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.*

*b. Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g., to cover such events as password aging).*

*c. Following loss management procedures to electronically unauthorize 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.*

*d. Use of transaction safeguards 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.*

*e. 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.*

- *Empower provides the ability to achieve compliance with this part of the rule.*
- *The software uses its own code to manage user ID and password for e-signature manifestations, removing the reliance on operating system and domain security.*
- *However, if the regulated company uses an LDAP authentication system such as Active Directory, Empower can be configured to use that system to manage usernames and passwords.*

*§11.300(a) No two individuals have the same combination of identification code and password.*

- Empower prohibits a user ID/password combination from being assigned to duplicate users. Even after a user is "removed" that ID cannot be reassigned.
- Despite these technical controls, it is the regulated company's responsibility to ensure that users do not share ID/password combinations between them.

*§11.300(b) System should force password changes periodically.*

- Empower allows an administrator to force a password change based upon company policy and business rules.

*§11.300(c) above is the user's responsibility; and falls under administrative/procedural controls.*

*§11.300(d) Ability to notify administrators of unauthorized system access attempts and lock the account after a specified number of failed attempts.*

- Empower provides this capability through its own code or through an LDAP solution such as Active Directory.
- In the event of more than a specified number of unsuccessful attempts to log in to Empower, the following will occur:
  - The user account is disabled, requiring an administrator to unlock.
  - Notification is sent to the Security Message Center, the System Audit Trail and, if configured, an email address.
  - This feature cannot be disabled.

§11.300 (e) Periodic testing of tokens or cards is not applicable to Empower.

## BEYOND THE RULE

### ASSISTANCE WITH AUDITS

Auditors require objective evidence to be provided in a timely fashion.

- Providing documented evidence becomes a fast, streamlined process when electronic data is online in the Empower database.
- Empower acts like an electronic filing cabinet. Instead of sifting through printed reports by hand, the Empower view filters can directly access the requested electronic data.

### MANAGE VALIDATION AND COMPLIANCE DOCUMENTATION

- Empower can be used to store qualification data and electronic reports for instruments and software in the lab.
- Since these checks need to be performed periodically, Empower provides not only a convenient storage location, but also a way of clearly documenting the timing of the various qualification tests done in the lab.
- Instrument and computer qualification status, including next qualification due dates, can be documented in the device properties.
- Validation and compliance data and reports are permanently stored within the relational database.
- Similar documentation libraries for non Empower controlled instrumentation can be created inside a secure relational database using Waters NuGenesis SDMS solution.

### ENSURING COMPLIANCE AND DATA INTEGRITY

Waters compliance experts are constantly reviewing regulatory observations as well as guidance documents and any regulation updates to ensure that the tools we provide

can help a regulated laboratory meet expectations for Data Integrity. It is important that responsible data owners understand and configure those tools correctly to meet

their own SOPs and requirements. Waters experts are available to provide training in the technical controls that Empower provides and how these might be leveraged.

*The information provided in this document is for informational purposes only and should not be construed as advice regarding any particular course of action to be taken by a particular reader. The information is subject to change without notice.*

*Waters does not make any representations or warranties, express or implied, to any party, regarding use of the information contained in this white paper to make decisions regarding the implementation and maintenance of effective quality control systems and quality assurance testing programs concerning the Chemistry Manufacturing and Controls activities with respect to products and operations conforming to appropriate best practices, including but not limited to the applicable good manufacturing practices regulations of the U.S. Food and Drug Administration or comparable regulations of any other supra-national, regional, federal, state, or local regulatory agency or authority that apply to the manufacture of pharmaceutical or biological products.*

For more information, reference www.fda.gov

## References

1. U.S. Food and Drug Administration. CFR – Code of Federal Regulations Title 21. FDA.gov. [Online] March 20, 1997, [Cited] October 26, 2012: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11.
2. European Commision Health and Consumers Directorate-General. European Commision. [Online] 01 2011, [Cited 10.26.12]: http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf.
3. U.S. Food and Drug Administration. Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance – Records and Reports. FDA.gov. [Online] August 3, 2010, [Cited] December 20, 2017: http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm#3.
4. U.S. Food and Drug Administration. Data Integrity and Compliance with CGMP Guidance for Industry, Level 2 DRAFT Guidance. FDA.gov. [Online] April 26, 2016, [Cited] December 20, 2017: https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm495891.pdf.
5. Medicines and Healthcare Products Regulatory Agency (MHRA). MHRA GXP Data Integrity Definitions and Guidance. Gov.UK. [Online] March 2018, [Cited] June 5, 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf.
6. Organization Economic Cooperation and Development (OECD). Principles of Good Laboratory Practice and Compliance Monitoring, Number 17. OECD.org. [Online] April 22, 2017, [Cited] December 20, 2017: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/jm/mono(2016)13&doclanguage=en.
7. U.S. Food and Drug Administration. Enforcement Policy: Electronic Records and Electronic Signatures Compliance Policy Guide, Guidance for FDA Personnel. FDA.gov. [Online] July 30, 1999, [Cited] December 20, 2017: https://www.fda.gov/ohrms/dockets/98fr/073099d.txt.
8. World Health Organization (WHO). Annex 5. Guidance on Good Data and Record Management Practices. [Online] 2016, [Cited] December 20, 2017: http://apps.who.int/medicinedocs/documents/s22402en/s22402en.pdf.

Waters

THE SCIENCE OF WHAT'S POSSIBLE.™

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
www.waters.com