[WHITE PAPER]

Waters
THE SCIENCE OF WHAT'S POSSIBLE.™

The Role of UNIFI Scientific Information System in Assisting with Electronic Records Regulation Compliance

INTRODUCTION

The objective of this white paper is to discuss the electronic record and Data Integrity compliance readiness of Waters™ UNIFI™ Scientific Information System 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,[1] 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, eventually e-record regulations will 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 an informatics platform 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 that is used in a regulated environment. A suite of technical controls for 21 CFR Part 11 and Annex 11 compliance are built into UNIFI 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 its European counterpart, the 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 Practice (GLP) and Good Clinical Practice (GCP)) as well as GMP, has transformed the management of electronic data in regulated life science industries.

Part 11 has serious overall implications for all aspects of regulated enterprise operations. No one technology or discipline is more or less affected by the rule; it is pervasive throughout an organization. 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 (HPLC, UPLC,™ GC, MS, NMR, GC-MS, etc.), Microsoft® Excel® and Word documents, Laboratory Information Management Systems (LIMS), Electronic Laboratory Notebooks (ELN), Scientific Data Management Systems (SDMS) and Laboratory Execution Systems (LES).

From the lab to the enterprise and beyond, Part 11 impacts good electronic record management significantly. The rule, originally proposed by the pharmaceutical industry to reduce the burden of paper submissions in 1991, became effective in August of 1997 for all companies wishing to sell food, pharmaceuticals, and cosmetics into the United States. Electronic record management and data integrity has 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 (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 re-use 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 every bit of 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. A Level 2 guidance[2] document was released on the www.fda.gov website in 2010 (and included in the more recent DRAFT guidance on Data Integrity[3]), specifically indicating that paper copies of electronic records from complex systems such as chromatographs will not meet 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.

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

- Work in a way that is compliant to regulators laws 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.
- Establish traceability between the human-readable data and the machine-readable data leveraging the capabilities of the built in relational database, Oracle.®

SUMMARY OF WATERS STRATEGIES FOR COMPLIANCE

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

In a Network, deployment data is stored in a secure central server, normally located in a server room (Figure 1), 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 do not have access to the raw data.

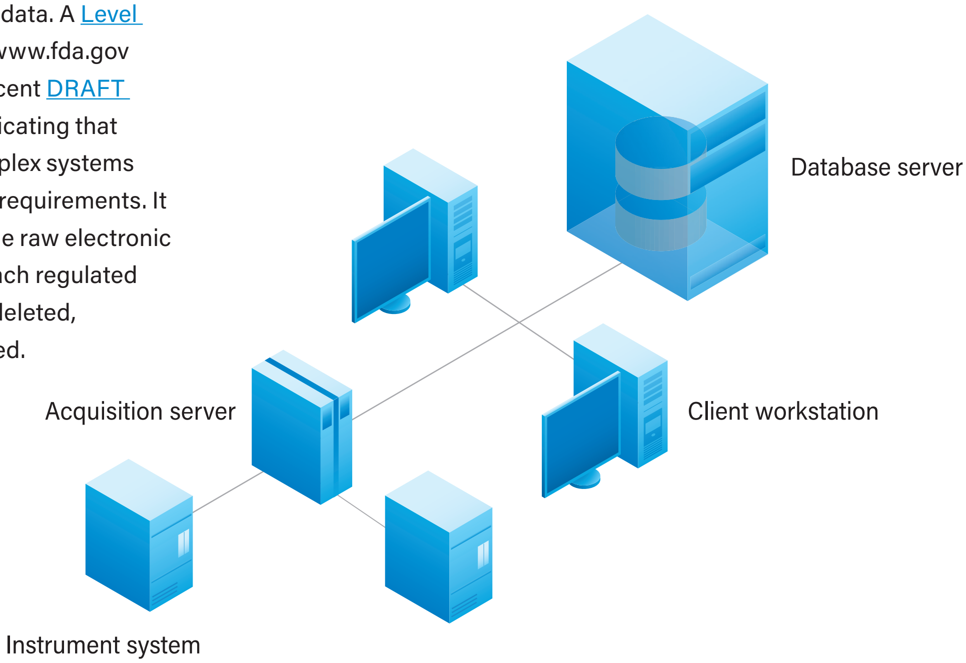


Figure 1. UNIFI in a Network configuration, showing the base Server, Clients and Laboratory Network Devices (LND) connected to an Instrument system.

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

UNIFI includes functionality which allows the regulated laboratory to simply configure and confidently demonstrate all of the technical requirements for electronic records as prescribed by 21 CFR Part 11, Annex 11 and other Data Integrity guidances. It 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.

PROTECTION AND READY RETRIEVAL OF RECORDS

All regulations expect that the original electronic data is protected, secured and available for review throughout the retention time of the record (based on the appropriate predicate rule). For FDA regulated companies section §11.10(c) of Part 11 applies.

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).

AUTOMATED BACKUP FOR DISASTER RECOVERY PURPOSES

Automated scripts can be set up and executed to provide electronic backups of the entire content of the UNIFI database and the associated files. A combination of backups and auto archive log files can restore UNIFI to the exact point of failure, should there be any serious hardware errors. There are huge benefits to having a central single database holding data from multiple instruments in the laboratory, on a server in a secure server room, and having one single set of scripts for automated backup of the entire lab's data.

EXPORT/ARCHIVE OF COMPLETED LABORATORY DATA

Archiving implies that data is moved from active state to inactive state and then be moved and stored long term in a new location. Key features for archiving data include:

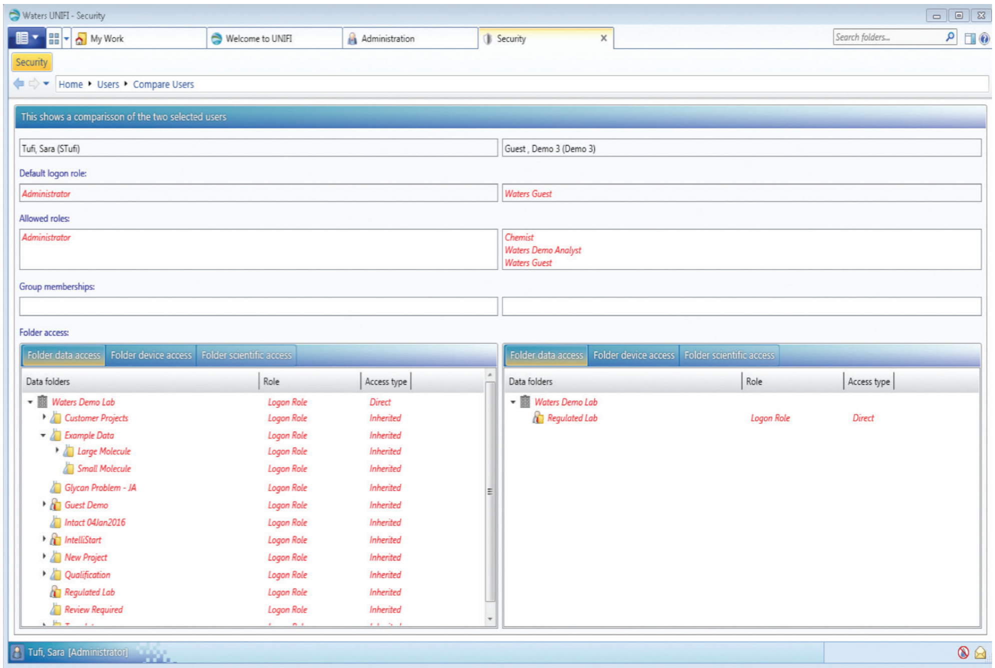
- Moving data, metadata, and audit trails to a secure storage area.
- Validation that the data migration preserves the relationships and integrity of the original data set.
- Technology to permit that data to be readily retrieved throughout the life of the data.
- It is not expected that these copies of data should be viewable in any application other than the original, or updated, version of the same application.
- It is imperative to capture the corresponding metadata along with the electronic record. UNIFI automatically creates electronic copies of all the metadata from both raw data and processed results in a folder, preserving all traceability between results and methods and stores this with the files, should you be required to remove it from your UNIFI network environment.
- Completed data in UNIFI may be secured by restricting the access to "Archive" folders using access controls, allowing access to only designated archivists or managers.
- UNIFI allows the raw data files to be automatically moved to a longer term storage area (using an offline storage manager (OSM)), while retaining the metadata in the central database for easy retrieval.
- UNIFI manages the archive process and provides a mechanism to export and archive several folders at one time.
- Easily retrieve archived data by using the restore function, which allows you to restore one or multiple folders.

LIMITING SYSTEM ACCESS

UNIFI 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 of "Attributable".

UNIFI is compliance-ready with these sub-sections provided the relevant access and system polices have been configured and suitable procedural and administrative controls are in place.

- UNIFI requires an authorized user login to gain access to the system. Once logged on, their role, as configured by an administrator, controls the user's access to data folders and scientific libraries. In this way data for different clients, for different studies, or different stages of completion can be managed. For instance, a dedicated folder tree may be used to secure completed and approved data folders such that it can be accessed only by the Study Director or Archivist (Figure 2).
- In a Network deployment, this type of access control extends to analytical instruments, LNDs, and client PCs.
- For enhanced records protection and access control, UNIFI assigns detailed permissions to user roles and users (i.e. not just read/write/delete access). For example, someone with pre-defined chemist permissions would only be allowed to sign reports for review, without the capability of approving them. Other permissions manage who can create, modify, delete, or allow/revoke access to specific content items such as data or methods (Figure 3).



This shows a comparisson of the two selected users

Tufi, Sara (STufi)	Guest , Demo 3 (Demo 3)

Default logon role:

Administrator	Waters Guest

Allowed roles:

Administrator	Chemist Waters Demo Analyst Waters Guest

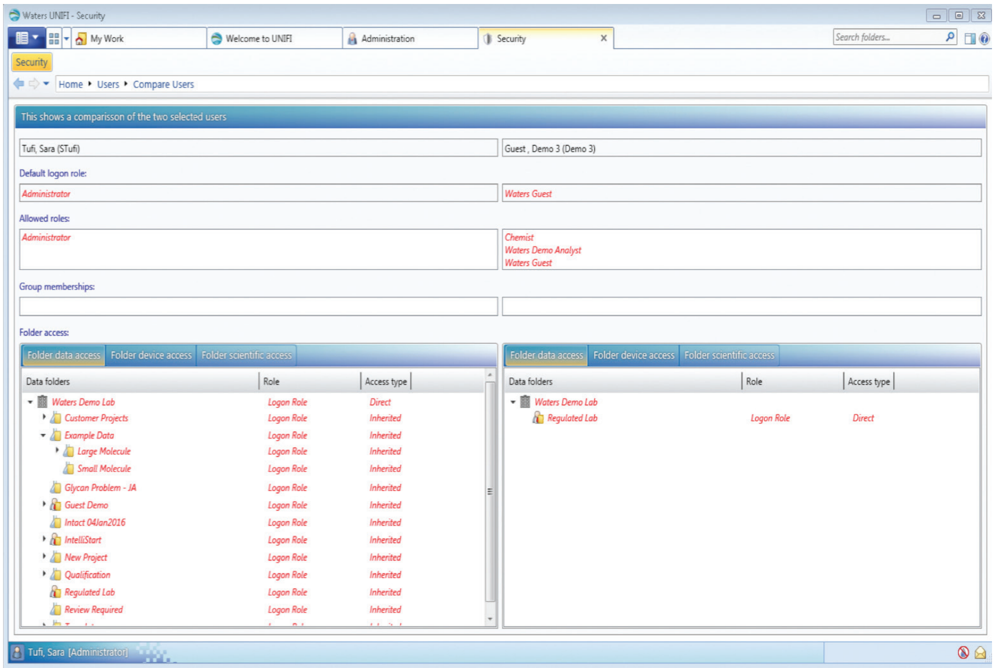
Group memberships:

Folder access:

Data folders	Role	Access type
Waters Demo Lab	Logon Role	Direct
Customer Projects	Logon Role	Inherited
Example Data	Logon Role	Inherited
Large Molecule	Logon Role	Inherited
Small Molecule	Logon Role	Inherited
Glycan Problem - JA	Logon Role	Inherited
Guest Demo	Logon Role	Inherited
Intact 04Jan2016	Logon Role	Inherited
IntelliStart	Logon Role	Inherited
New Project	Logon Role	Inherited
Qualification	Logon Role	Inherited
Regulated Lab	Logon Role	Inherited
Review Required	Logon Role	Inherited

Data folders	Role	Access type
Waters Demo Lab		
Regulated Lab	Logon Role	Direct

Figure 2. User comparison highlights the different user roles and access to selected folders.



This shows a comparisson of the two selected users

Tufi, Sara (STufi)	Guest , Demo 3 (Demo 3)

Default logon role:

Administrator	Waters Guest

Allowed roles:

Administrator	Chemist Waters Demo Analyst Waters Guest

Group memberships:

Folder access:

Data folders	Role	Access type
Waters Demo Lab	Logon Role	Direct
Customer Projects	Logon Role	Inherited
Example Data	Logon Role	Inherited
Large Molecule	Logon Role	Inherited
Small Molecule	Logon Role	Inherited
Glycan Problem - JA	Logon Role	Inherited
Guest Demo	Logon Role	Inherited
Intact 04Jan2016	Logon Role	Inherited
IntelliStart	Logon Role	Inherited
New Project	Logon Role	Inherited
Qualification	Logon Role	Inherited
Regulated Lab	Logon Role	Inherited
Review Required	Logon Role	Inherited

Data folders	Role	Access type
Waters Demo Lab		
Regulated Lab	Logon Role	Direct

Figure 3. Comparing roles enables quick review and/or modification of user roles and their associated permissions. Permissions which are not common between the roles compared appear in red.

If multiple roles have been assigned to a user, during login the user can choose which role to access UNIFI with the appropriate access they need for that session (Figure 4).

DEVICE MANAGEMENT

§11.10(h) Describes "device checks" and uses the example of terminal as a point of entry of data. For UPLC-MS solutions it is more applicable to consider devices as chromatography and mass spectrometry instruments, which are the main sources of data input.

UNIFI will capture data from any instrument system or device that the user specifies. A valid instrument driver and license (in a Network environment) need to be installed, and the specific instrument system must be configured in UNIFI. User access to a device is controlled by the software using role and access type, as described above.

As well as directly controlled LC, GC, and MS instruments, UNIFI can collect data from any device that will output an analog signal into a convertor called an eSAT/IN. This data will be transferred to UNIFI and can be processed just as if it came from a directly controlled instrument. This can be useful to monitor other output signals from non-controlled instruments.

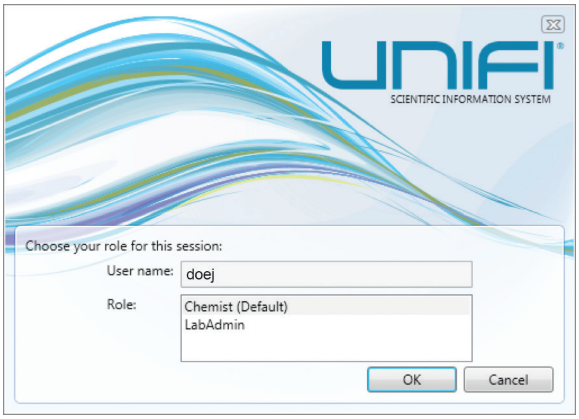
Qualification of instruments and eSAT/IN devices will help show adherence to this section of the rule, as well as complying with other GMP and GLP regulations regarding calibration or checking of equipment.

AUDIT TRAILS

The use of computer generated, time-stamped audit trails are a significant part of the 'Controls for Closed Systems.' (§11.10(e)) 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.

As stated in the April 2016 OECD Guidance Number 17 for Applications of GLP Principles to Computerized Systems[4]: "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 product quality. The absence of an audit trail is considered to be, "highly significant when there are data discrepancies" according to the FDA.[5]



Choose your role for this session:

User name: doej

Role: Chemist (Default)
LabAdmin

Figure 4. A user choosing the role appropriate for this session.

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.

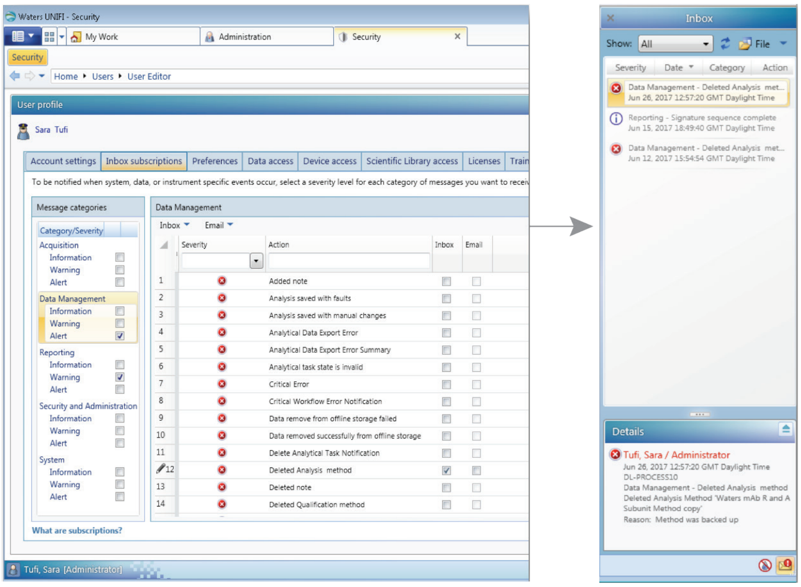
By default, audit trails are enabled in UNIFI. The audit trails are generated automatically and its functionality can never be switched off. Users may configure Reasons for Change requirements to suit their working needs and meet their compliance requirements.

UNIFI has an Event Log which automatically tracks system-level and user-generated activities using secure, time-and-date stamped event log/audit trail records. These records are automatically stored in the database and viewable to you as messages in a table format on the Event Log tab.

There are a number of Event log views built into UNIFI to help search for the most relevant records:

- Event Browser – All Messages.
- System Audit Trail – System-generated and Security and Administration messages only – such as denied login, project archival, changes to system policies, and user/role permissions.
- Data Audit Trail – Messages regarding activities with items such as items, methods, files, folders, and data only.

All UNIFI users can individually select the kind of notifications that will be delivered to their UNIFI Inbox (Figure 5), by subscribing to specific notifications, including certain severity of messages or very specific audit trail records (e.g. Modified Analysis Method).



To be notified when system, data, or instrument specific events occur, select a severity level for each category of messages you want to recei

Category/Severity	
Acquisition	
Information	□
Warning	□
Alert	□
Data Management	
Information	□
Warning	□
Alert	☑
Reporting	
Information	□
Warning	☑
Alert	□
Security and Administration	
Information	□
Warning	□
Alert	□
System	
Information	□
Warning	□
Alert	□

	Severity	Action	Inbox	Email
1	⊗	Added note	□	□
2	⊗	Analysis saved with faults	□	□
3	⊗	Analysis saved with manual changes	□	□
4	⊗	Analytical Data Export Error	□	□
5	⊗	Analytical Data Export Error Summary	□	□
6	⊗	Analytical task state is invalid	□	□
7	⊗	Critical Error	□	□
8	⊗	Critical Workflow Error Notification	□	□
9	⊗	Data remove from offline storage failed	□	□
10	⊗	Data removed successfully from offline storage	□	□
11	⊗	Delete Analytical Task Notification	□	□
12	⊗	Deleted Analysis method	☑	□
13	⊗	Deleted note	□	□
14	⊗	Deleted Qualification method	□	□

Severity	Date	Category	Action
⊗	Data Management - Deleted Analysis met... Jun 26, 2017 12:57:20 GMT Daylight Time		
ⓘ	Reporting - Signature sequence complete Jun 15, 2017 18:49:40 GMT Daylight Time		
⊗	Data Management - Deleted Analysis met... Jun 12, 2017 15:54:54 GMT Daylight Time		

Tufi, Sara / Administrator
Jun 26, 2017 12:57:20 GMT Daylight Time
DL-PROCESS10
Data Management - Deleted Analysis method
Deleted Analysis Method 'Waters mAb R and A Subunit Method copy'
Reason: Method was backed up

Figure 5. Showing both Inbox Subscription set up and specific notification messages/Audit Trail records pushed to a user's UNIFI Inbox.

Data Audit Trails captures information that affects all data (calibration, method changes, processing data) and other information captured in UNIFI database (who, when, what), including any data insertions, modifications to metadata, record copies, deletions, generation of reports (in PDF or paper format), and applications of review or approval signatures following the associated signature workflow.

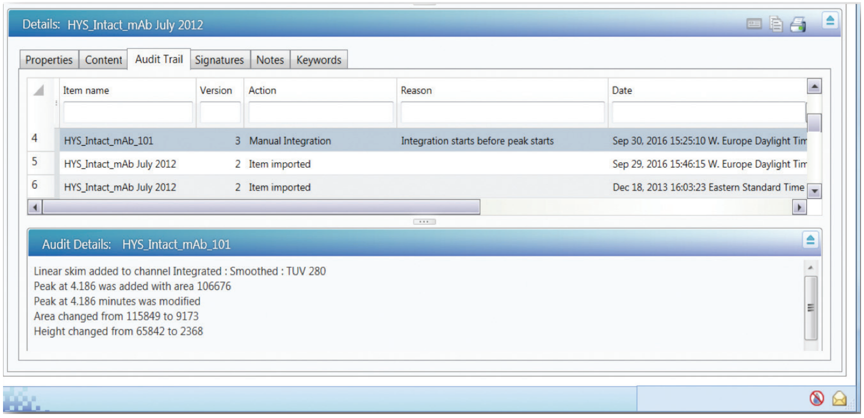
Data Audit Trails are permanently associated with the data they relate to, leveraging the relational database, and will follow the data if it is archived or moved.

In Figure 6, the analysis audit trail is capturing a manual integration. More detailed information can be found for each action performed/line in the audit trail under the Audit Details. Here related information such as the user credentials, the time stamp, the item type, the analysis version number, and importantly, the reason for change that the user has entered.

For each item type (i.e. raw data, process data, report, report template, etc.) UNIFI keeps track of all versions. A full version history is stored for a specific item, such as a method, and earlier versions can be retrieved and displayed at any time. In addition, the audit trail keeps track of changes which occurred throughout the whole data history, providing the details needed to reconstruct the story of the data.

Old versions of analyses can be opened and available for review and further processing, ensuring that all the historical data and information are always available.

Old versions of methods can be opened and available for review and may be used to acquire or process new data.

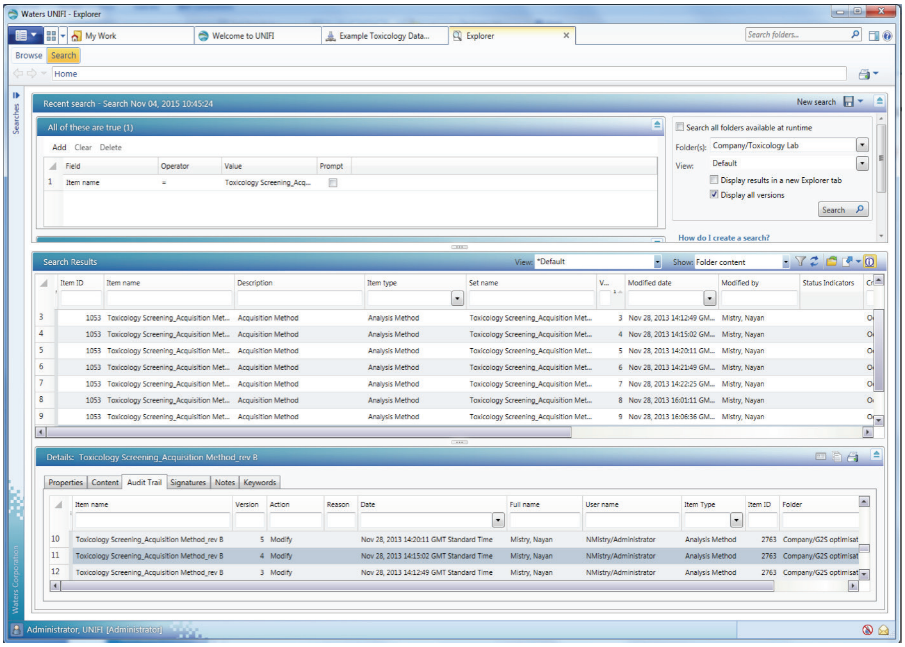

Details: HYS_Intact_mAb July 2012
Properties
Content
Audit Trail
Signatures
Notes
Keywords
Audit Details: HYS_Intact_mAb_101

	Item name	Version	Action	Reason	Date
4	HYS_Intact_mAb_101	3	Manual Integration	Integration starts before peak starts	Sep 30, 2016 15:25:10 W. Europe Daylight Tim
5	HYS_Intact_mAb July 2012	2	Item imported		Sep 29, 2016 15:46:15 W. Europe Daylight Tim
6	HYS_Intact_mAb July 2012	2	Item imported		Dec 18, 2013 16:03:23 Eastern Standard Time

Linear skim added to channel Integrated : Smoothed : TUV 280
Peak at 4.186 was added with area 106676
Peak at 4.186 minutes was modified
Area changed from 115849 to 9173
Height changed from 65842 to 2368

Figure 6. Showing the high level and detailed Audit Trail for this chromatogram.

The relational database keeps track of which versions of methods are associated with which data, even if those methods have been modified and used for other sets of data subsequently (Figure 7).



Recent search - Search Nov 04, 2015 10:45:24

All of these are true (1)

	Field	Operator	Value	Prompt
1	Item name	=	Toxicology Screening_Acq...	□

□ Search all folders available at runtime
Folder(s): Company/Toxicology Lab
View: Default
□ Display results in a new Explorer tab
☑ Display all versions
Search
How do I create a search?

Search Results View: *Default Show: Folder content

	Item ID	Item name	Description	Item type	Set name	V...	Modified date	Modified by	Status Indicators	Cr
3	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	3	Nov 28, 2013 14:12:49 GM...	Mistry, Nayan		O
4	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	4	Nov 28, 2013 14:15:02 GM...	Mistry, Nayan		O
5	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	5	Nov 28, 2013 14:20:11 GM...	Mistry, Nayan		O
6	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	6	Nov 28, 2013 14:21:49 GM...	Mistry, Nayan		O
7	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	7	Nov 28, 2013 14:22:25 GM...	Mistry, Nayan		O
8	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	8	Nov 28, 2013 16:01:11 GM...	Mistry, Nayan		O
9	1053	Toxicology Screening_Acquisition Met...	Acquisition Method	Analysis Method	Toxicology Screening_Acquisition Met...	9	Nov 28, 2013 16:06:36 GM...	Mistry, Nayan		O

Details: Toxicology Screening_Acquisition Method_rev B

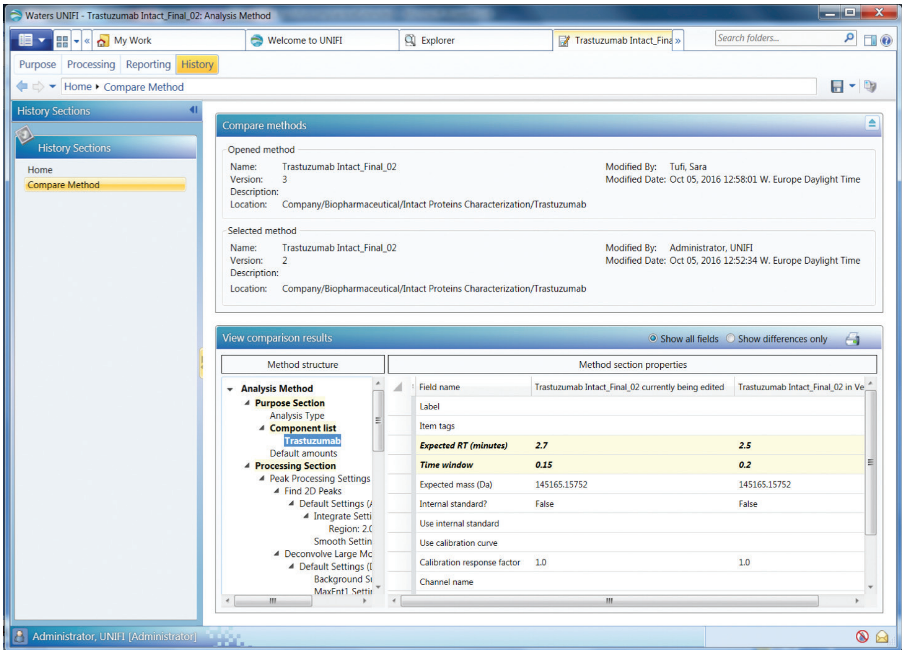
Properties | Content | Audit Trail | Signatures | Notes | Keywords

	Item name	Version	Action	Reason	Date	Full name	User name	Item Type	Item ID	Folder
10	Toxicology Screening_Acquisition Method_rev B	5	Modify		Nov 28, 2013 14:20:11 GMT Standard Time	Mistry, Nayan	NMistry/Administrator	Analysis Method	2763	Company/G2S optimisat
11	Toxicology Screening_Acquisition Method_rev B	4	Modify		Nov 28, 2013 14:15:02 GMT Standard Time	Mistry, Nayan	NMistry/Administrator	Analysis Method	2763	Company/G2S optimisat
12	Toxicology Screening_Acquisition Method_rev B	3	Modify		Nov 28, 2013 14:12:49 GMT Standard Time	Mistry, Nayan	NMistry/Administrator	Analysis Method	2763	Company/G2S optimisat

Administrator, UNIFI [Administrator]

Figure 7. Searching for a specific method and showing time stamped versions demonstrating the history.

Different versions of the same analysis method or different analysis methods can be compared in a UNIFI tool which automatically highlights the fields that have been changed. This might be comparing one version to the other (whether consecutive or not) or from one analysis method to another completely different analysis method. One use for this comparison would be to ensure that analysts are only making changes to specific parameters as specified in a Standard Operating Procedure (SOP). Any parameters that are different are clearly highlighted for the viewer as is shown in Figure 8.



Compare methods

Opened method
Name: Trastuzumab Intact_Final_02
Version: 3
Description:
Location: Company/Biopharmaceutical/Intact Proteins Characterization/Trastuzumab
Modified By: Tufi, Sara
Modified Date: Oct 05, 2016 12:58:01 W. Europe Daylight Time

Selected method
Name: Trastuzumab Intact_Final_02
Version: 2
Description:
Location: Company/Biopharmaceutical/Intact Proteins Characterization/Trastuzumab
Modified By: Administrator, UNIFI
Modified Date: Oct 05, 2016 12:52:34 W. Europe Daylight Time

View comparison results ● Show all fields ○ Show differences only

Method structure

- **Analysis Method**
  - **Purpose Section**
    - Analysis Type
    - **Component list**
      - Trastuzumab
    - Default amounts
  - **Processing Section**
    - Peak Processing Settings
      - Find 2D Peaks
        - Default Settings (/
          - Integrate Setti
            - Region: 2.(
          - Smooth Settin
      - Deconvolve Large Mc
        - Default Settings (I
          - Background Si
          - MaxEnt1 Settii

Method section properties

Field name	Trastuzumab Intact_Final_02 currently being edited	Trastuzumab Intact_Final_02 in Ve
Label		
Item tags		
Expected RT (minutes)	***2.7***	***2.5***
Time window	***0.15***	***0.2***
Expected mass (Da)	145165.15752	145165.15752
Internal standard?	False	False
Use internal standard		
Use calibration curve		
Calibration response factor	1.0	1.0
Channel name		

Administrator, UNIFI [Administrator]

Figure 8. Methods can be quickly compared to facilitate the review of the modification history, with the differences automatically highlighted in yellow.

While UNIFI is tracking every change made to methods and data via the application, it also provides Checksum and Cyclic Redundancy Check (CRC) verification for all human-readable and machine-readable data to protect against data being altered by external access to the system.

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 administrator's SOP.

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[6] notes that 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. There is no expectation for documenting separately the review of audit trails.

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:

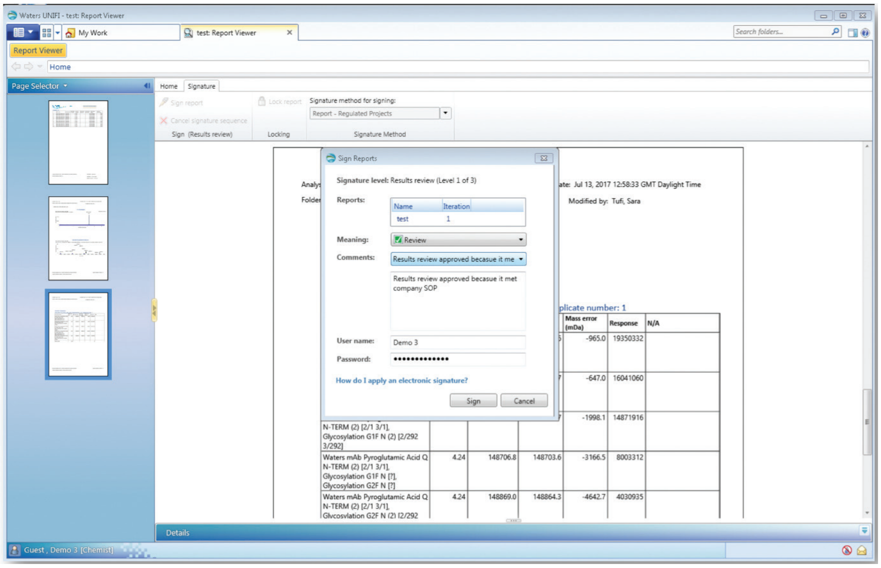
- User ID and password
- Card key and password
- Two passwords

"§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.*
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."*

UNIFI has been developed with many enhanced features for managing signature workflows:

- Provides the ability to achieve compliance with this part of the Rule.
- Requires a unique username/password combination in order to e-sign an individual or summary report (Figure 9).
- Ensures that all pages of the report are reviewed before sign off is permitted.
- Single signatures can be applied simply or sophisticated signature workflows which can be created and saved.
- PDFs of the actual report used for signature are automatically stored.
- Signed reports can also be printed to NuGenesis™ SDMS or sent via email.



Signature method for signing: Report - Regulated Projects

Signature level: Results review (Level 1 of 3)

Reports:

Name	Iteration
test	1

Meaning: Review

Comments: Results review approved becasue it me

Results review approved becasue it met company SOP

User name: Demo 3

Password: ••••••••••••••

How do I apply an electronic signature?

ate: Jul 13, 2017 12:58:33 GMT Daylight Time

Modified by: Tufi, Sara

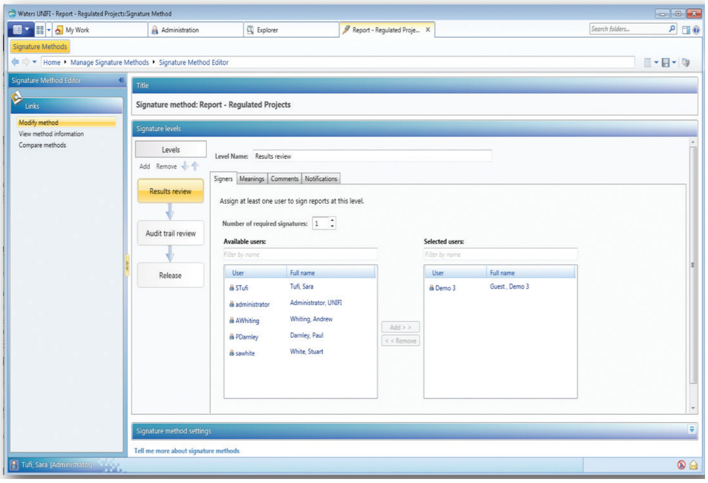
				Mass error (mDa)	Response	N/A
				-965.0	19350332	
				-647.0	16041060	
N-TERM (2) [2/1 3/1], Glycosylation G1F N (2) [2/292 3/292]				-1998.1	14871916	
Waters mAb Pyroglutamic Acid Q N-TERM (2) [2/1 3/1], Glycosylation G1F N [?], Glycosylation G2F N [?]	4.24	148706.8	148703.6	-3166.5	8003312	
Waters mAb Pyroglutamic Acid Q N-TERM (2) [2/1 3/1], Glvcosvlation G2F N (2) [2/292	4.24	148869.0	148864.3	-4642.7	4030935	

Figure 9. Applying a unique electronic signature to a report, showing the meaning and additional comments, as well as the application of the two part electronic signature.

SIGNATURE METHODS

UNIFI allows laboratories to establish a review and approval process for reports using a signature method. A signature method defines a series of review phases, called levels. You can assign any name you want to each review level and specify the sequence in which to complete each level in the overall review process (Figure 10).

- Signature requests/notifications can be sent to a group of users and may require either one or more than one of the group to sign before moving to the next signature level.
- Permission-based controls around who can sign results at each level, with multiple configurable signature levels available.
- Due dates can be assigned for each signature level.
- Prompt users when signature are due through the My Work tab.



Signature method: Report - Regulated Projects

Level Name: Results review

Assign at least one user to sign reports at this level.

Number of required signatures: 1

Available users:

User	Full name
STufi	Tufi, Sara
administrator	Administrator, UNIFI
AWhiting	Whiting, Andrew
PDarnley	Darnley, Paul
sawhite	White, Stuart

Selected users:

User	Full name
Demo 3	Guest , Demo 3

Figure 10. This screenshot shows an example Signature Method with multiple configurable signature levels and authorized users who may sign at that level, clearly indicating the reason for that signature.

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 of the reviewer who approves the data. However, many companies will have their own SOPs about how records are reviewed and approved.

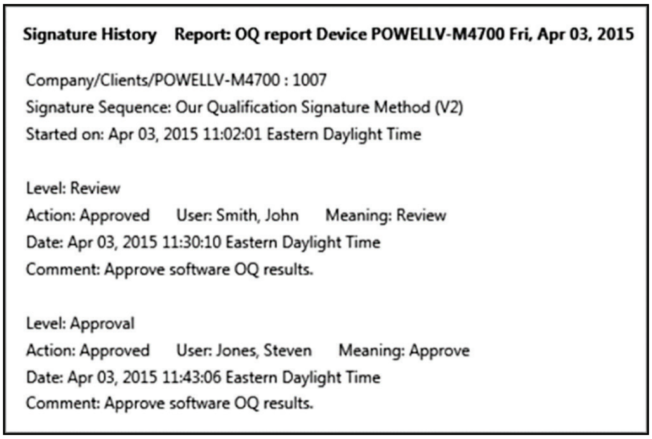
The US regulation does, however, require e-signature manifestations to contain three key pieces of metadata. It is stated that:

"(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*
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)."

- UNIFI 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. In addition option comments may be included at this point.
- UNIFI e-signature displays as part of the report:
  - The full name of the signer
  - The date and the time that the signature was executed
  - A meaning for the signature plus additional optional comments
  - The signature information may be inserted on a separate page, before the first page of the report, or after the last page of the report (Figure 11).



Signature History **Report: OQ report Device POWELLV-M4700 Fri, Apr 03, 2015**

Company/Clients/POWELLV-M4700 : 1007
Signature Sequence: Our Qualification Signature Method (V2)
Started on: Apr 03, 2015 11:02:01 Eastern Daylight Time

Level: Review
Action: Approved User: Smith, John Meaning: Review
Date: Apr 03, 2015 11:30:10 Eastern Daylight Time
Comment: Approve software OQ results.

Level: Approval
Action: Approved User: Jones, Steven Meaning: Approve
Date: Apr 03, 2015 11:43:06 Eastern Daylight Time
Comment: Approve software OQ results.

Figure 11. In the electronic signature the user credentials will be printed as well as the meaning for approval/rejection and additional comments.

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

UNIFI prevents:

- Re-allocation of e-signatures to another user.
- Deletion of a user/signer once it has been created and used, creating a permanent record of that user and preventing the same user name/signature being used by a new user.

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.

- UNIFI provides the ability to achieve compliance with this part of the rule.
- The software enables non-breakable linking of electronic signatures to electronic records.
- UNIFI e-signature information is stored in the Oracle relational database and is permanently linked to the report itself.
- It is not possible to excise, copy, or transfer the signature to another unsigned document.
- Once data report has been signed, signatures cannot be removed.
- Although the report, rather than the result, is signed, the relational database permanently associates that signature with all associated results.

CONTROLS FOR IDENTIFICATION CODES/ PASSWORDS (§11.300):

Ultimately, the purpose of Part 11, Annex 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.*

- UNIFI 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.

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

- UNIFI prohibits a user name/password combination from being assigned to duplicate users. Even after a user is "removed" that user name cannot be reassigned to a new user.
- 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.

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

§11.300(c) Confirming the users true identity is the companies' 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.

- In the event of more than a specified number of unsuccessful attempts to log in to UNIFI, the following will occur:
  - The user account is disabled, requiring an administrator to unlock.
  - Notification is sent to the Event Log and additionally to any User who has subscribed to receive notifications about incorrect log on attempts and/or User account disablement.
  - This feature cannot be disabled.
- User accounts can be configured with a specified expiration date and allows an "inactivity" time period to be set which might automatically lock an unused account.

BEYOND THE RULE

ASSISTANCE WITH AUDITS

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

- If analytical reports are online in the UNIFI database, providing documented evidence becomes a fast, streamlined process.
- Instead of sifting through printed reports by hand, the Software Quick Search can access the requested report quickly. This software functionality enables keyword searching among all of the data stored in the Oracle database, leveraging their relationships.
- Other PDFs can also be stored associated with the data, for example: training records, SOPs, material safety data sheets, and method monographs. These items would be searchable and available during an audit.
- UNIFI provides a single integrated solution so data does not need to be moved between software platforms.

MANAGE VALIDATION AND COMPLIANCE DOCUMENTATION

- UNIFI can be used to store installation and operational qualification data and electronic reports for instruments and software in the lab.
- Since these checks need to be performed periodically, UNIFI 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, are managed in the Qualification and Maintenance Center.

- Users and Engineers can record maintenance activities and supporting documentation in the Qualification and Maintenance Center and link these to qualification actions.
- Validation and compliance data and reports are permanently stored within the relational database. UNIFI permits Engineers or other individuals performing maintenance or qualification to store documents, such as training records or other objective evidence in the Qualification and Maintenance Center.

ENSURING COMPLIANCE AND DATA INTEGRITY

Waters compliance experts regularly review regulatory observations as well as guidance documents and any regulation updates to ensure the tools we provide help a regulated laboratory meet expectations for Data Integrity. It is important that responsible data owners understand and configure these tools correctly to meet their own SOPs and requirements. Waters experts are available to provide training in the technical controls that UNIFI 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, expressed 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. Administration, U.S. Food and Drug. 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.
3. Administration, U.S. Food and Drug. 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.
4. 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.
5. 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.
6. 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