Ensuring Regulatory Compliance to 21 CFR Part 11 with Empower 2 Enterprise Network solutions

Use and management of electronic records meets the FDA expectation
You Cannot Just ‘Buy’ a Compliant System

Compliant Ready Software
- Software designed with compliance in mind
  - Full audit trail
  - Easy set up in system policies
  - Easy to retrieve/view off-line

Procedural Controls are needed too
- Unique accounts and secret passwords
- Regular backups
- OS and Physical security
## Compliance Requirements:
### System Set Up and Policies

<table>
<thead>
<tr>
<th><strong>Workstation</strong></th>
<th><strong>Client Server</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data stored on PC in the lab</td>
<td>Data only stored on server in secured server room</td>
</tr>
<tr>
<td>PC hardware failures result in loss of data</td>
<td>RAID technology protects from failure</td>
</tr>
<tr>
<td>Expensive to licence a username for every analyst on every workstation</td>
<td>One user licence for every instrument in the lab</td>
</tr>
<tr>
<td>Many user names and passwords to maintain</td>
<td>Single set of passwords</td>
</tr>
<tr>
<td>Time Stamps from unsecured PC time</td>
<td>Time Stamps from the Server</td>
</tr>
<tr>
<td>Access to OS (task manager/explorer) on PC compromises security of data</td>
<td>Access to OS of PC does not compromise data security</td>
</tr>
<tr>
<td>SOP’s’ need to synchronize naming conventions (files, methods, e-records)</td>
<td>Single data repository ensures uniqueness of ID’s</td>
</tr>
</tbody>
</table>
Purpose of 21 CFR Part 11

- To make electronic recordkeeping:
  - Trustworthy
  - Reliable
  - Compatible with the FDA’s public health protection responsibilities

- The ground rules for paving the way to full electronic submission to CA, EU, US and JA in the Future – e-CTD

- Regulation is on the books and being enforced using risk management
Chapter 21 Code of Federal Regulations

21 CFR Part 211 - Current Good Manufacturing Practice for Pharmaceutical Products

21 CFR Part 58 - Current Good Laboratory Practice for Pharmaceutical Products

21 CFR Part 110 - Current Good Manufacturing Practice in Manufacturing Packing or Holding of Human Food

21 CFR Part 820 - Quality System Regulation for Medical Devices
FDA Predicate Rules for Records Management

- **21 CFR 211.194 Laboratory Records**
- 21 CFR 58.185, 58.190, 58.195 Records and Reports
- 40 CFR 160.185, 160.190, 160.195 Records and Reports
- 21 CFR 113.100 & 114.100 Records and Reports
- 21 CFR 820.180-198 Records
- 21 CFR 312.57 and 312.62 Record Keeping and Retention
- 21 CFR 11.10 (b,c,e,k) Electronic Records
21 CFR Part 211: What records need to be kept?

- § 211.182 Equipment cleaning and use log.
- § 211.184 Component, drug product container, closure, and labeling records.
- § 211.186 Master production and control records.
- § 211.188 Batch production and control records.
- § 211.192 Production record review.
- § 211.194 Laboratory records.
- § 211.196 Distribution records.
- § 211.198 Complaint files.
21 CFR Part 211.194: Laboratory Records

All records required to be kept

Lab Book or forms

Various PC’s in Lab

Analytical Applications or Excel

Lab Book or forms
As with FDA regulations, the Eu GMP regulations have predicate rules (Chapters) overlaid with the electronic record rule (Annex 11)

Major difference to date
- FDA has maintained that if you use electronic records for regulatory activity (i.e., calculating things) this is your raw data
  - You cannot define paper in this case
- Eu Regulation always allow the choice
  - If you like, delete the e-records rely on the paper ones
  - New draft Annex 11 questions this for complex systems
Future Changes to the Scope of Part 11?

- New guidance suggests some leniency during inspections in the short term
  - legacy systems (pre August 20th 1997 - pre Y2K?)
  - low risk systems that you decide will still be paper based
  - systems where the paper version can be used to perform necessary regulated activities
e.g. SOP’s written in word and the printed version is always used
  - long term archive, e-copies and reprocessability
Future Changes to the Scope of Part 11?

- While the **1997 rule is still law**, there will be a **review** of the **scope** of Part 11...
- Laboratory analytical software is high risk and the e-record is used to generate the batch data
  - So new scope is **not expected** to affect status of laboratory analytical software e-records
Printouts of Electronic Records

- The printed hardcopy is a “temporary representation”.
- It cannot be guaranteed without e-records compliance.
- This includes a print to paper or a print to PDF
  - You must record the meta data
  - Where are the audit trails in a paper record or in a PDF?
- Agency may ask you to re-create report from the electronic record.
- .....even if your “final” data is in paper format with a handwritten signature (like at Able).

“More about the record than what’s on paper; The Electronic Record is the Master”
Key Topics of Part 11

- **Secure Records**
  - Back up, archive, records retention policy of ALL data and metadata
  - Easy retrieval of e-records and HumanReadable copies
  - Controlled access with unique username and password
    - limit functionality
    - feeds audit trail
  - Secure computer generated audit trails for any changes to data
    - What changed, who, when why (and now where)

- **Applications that work**
  - Validation
  - Training

- **Electronic Signatures**
  - Non repudiation of signature (if using)
Your firm has not exercised appropriate controls over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel [21 CFR 211.68(b)].

- For example, your firm lacks systems to ensure that all electronic data generated in your Quality Control laboratory is secure and remains unaltered. **All analysts have system administrator privileges that allow them to modify, overwrite, and delete original raw data files** ... in the High Performance Liquid Chromatography (HPLC) units.

- In addition, your firm's **review of laboratory data does not include a review of an audit trail** or revision history to determine if unapproved changes have been made.
Your firm has not exercised appropriate controls over computer or related systems to assure that changes in control records or other records are instituted only by authorized personnel [21 CFR § 211.68(b)].

For example, one user account is established for two analysts to access the laboratory instrument's software on the computer system attached to HPLC systems.

The user account provides full system administrative rights, including editing of the methods and projects.

In addition, data security protocols are not established that describe the user's roles and responsibilities in terms of privileges to access, change, modify, create, and delete projects and data.
Appropriate controls are not exercised over computers or related systems to assure that changes in analytical methods or other control records are instituted only by authorized personnel [21 CFR 211.68(b)].

b) User access levels for the software were not established and documented. Currently, laboratory personnel use a common password to gain access to the system and there are no user access level restrictions for deleting or modifying data. Furthermore, your system does not have an audit trail to document changes.
3. **Failure to adequately validate** the intended use of this PC and its software, as required by 21 CFR 820.70(i).

   - "For example: the dedicated PC [redacted] attached to the [redacted] was not secure in that
     - access to the data on [redacted] was not granted by a unique username and password or equivalent method;
     - there as no documentation associated with the electronic data for whom was responsible for collection of the analytical results as several quality control personnel have access to the [redacted]
     - no software changes in the study data could be detected as there was no audit trail capability;
     - the electronic data did not correlate with the paper records."
Failure to establish adequate controls and procedures to assure the authenticity, integrity, and security of all electronic records including data generated in the laboratory as required by 21 CFR § 211.68(b).

- **System administrator** privileges were to be assigned to validation chemists, lead chemists, and laboratory supervisors only. Our investigators documented numerous instances where these privileges were reassigned to other chemists without documentation or justification some of which resulted in extensive manipulation of data with no explanation regarding why the manipulation was conducted.

- These manipulations would include changing integration parameters or re-labeling peaks such that previously resolved peaks would not be integrated and included in the calculation for impurities.
This **intentional data manipulation** included using standards from a different run, changes to the concentration of the standards, changes to the number of capsules tested, changes in multipliers, changes in sample weights, and changes in dissolution volumes.

Although the audit function is discussed in your procedures, your records failed to include documentation that a second person had conducted such a review. In fact, our investigator was told that **no such audit had ever been performed**.

A second person must review these audit trails, particularly given the lack of controls for preventing data manipulation. **Such an audit may well have detected the data manipulation which was occurring at your facility.**
### Product / Batch Number

<table>
<thead>
<tr>
<th>Product / Batch Number</th>
<th>Lack of Complete Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products and batches listed in FDA-483, point # 2</td>
<td>OOS results not documented in laboratory records. Unreported OOS results found in electronic data files.</td>
</tr>
<tr>
<td>Propoxyphene Napsylate and APAP Tablets, 100/650mg Batch 303110A</td>
<td>Changed chromatogram headers by cutting and pasting, so during review all sample injections would appear to be in sequence, for Dissolution Testing of Tablets D1 and D5.</td>
</tr>
<tr>
<td>Propoxyphene Napsylate and APAP Tablets, 100/650mg Batch 104026B Validation Batch</td>
<td>Original Sample Weights not recorded in notebook. Sample weights were changed by the analyst until a passing result was obtained for Assay (A2)</td>
</tr>
<tr>
<td>Acetaminophen &amp; Codeine Phosphate Tablets, 300/30mg Batch 407148</td>
<td>Processing methods changed by analyst until the processing method resulted in a passing result. Original processing method not recorded in laboratory notebook.</td>
</tr>
</tbody>
</table>
3. Failure to employ appropriate controls over computer or related systems... [21 CFR § 211.68(b)]

For example, your firm has inadequate security measures in place to assure the integrity and reliability of data generated by your laboratory.

During the December 2005 inspection, our investigators observed your laboratory analysts operating computers under different analysts' names. Your analysts told our investigators that using other laboratory personnel's names and passwords was a common occurrence in your firm's laboratory while using your Turbochrom laboratory software.
• Failure to have a **validated and secure** computerized system. Additionally, there were no written protocols to assign levels of responsibilities for the system.

  — It was noted that the [redacted] instrument model [redacted] used for the analysis of [redacted] failed to have **password control** for the analysts and the supervisor. It was observed that the **data stored on the computer can be deleted**, removed, transferred, renamed or altered.

• Please note that computerized systems should have sufficient controls to prevent unauthorized access or changes to data. There should be controls to prevent data omissions and assure back-up. There should be a record of **any data change made, the previous entry, who made the change, and when the change was made**.
the laboratory is using an electronic record system for processing and storage of data from the atomic absorption and HPLC instruments that is not set up to control the security and data integrity in that the system is
- not password controlled,
- no systematic back-up provision, and there is
- no audit trail of the system capabilities.

The system does not appear to be designed and controlled in compliance with the requirements of 21 CFR Part 11, Electronic Records.
The data acquisition system for the UV/Visible spectrophotometers allows your analysts to **modify, overwrite, and delete original raw data files**... All laboratory personnel were given roles as Managers, which allowed them to modify, delete, and overwrite results files.

This system also does not include an **audit trail** or any **history of revisions** ...

Your laboratory computer system lacks necessary controls to ensure that data is protected from tampering, and it also lacks audit trail capabilities to detect data that could be potentially compromised."
- Specifically, your firm creates and stores all written information as electronic files and you do not keep any hard copies of these records.

- Your electronic documentation system does not meet **system validations, system access limitations, audit trails, signature manifestations, and signatures to record linking requirements** to ensure they are trustworthy, reliable and generally equivalent to paper records as required by **21 CFR Part II**.
Summary of findings

- No Secure Access to only authorized personnel
  - No password
  - Shared users accounts
    - Set up that way
    - Shared in an emergency without documentation or justification
- No controls to limit access to the delete function (among others)
  - Either set up as administrators
  - Or with user types that permit deletion or data manipulation
- No Audit trails
  - Software not equipped with Audit trail
  - Users not having unique log on prevents correct audit trails
  - No REVIEW of audit trails by managers / QA
Empower System Policies

How do they help you comply to 21 CFR Part11?
Empower Software Security

- Windows (2000 or XP) operating system software is only used to secure the database and raw data records from accidental deletion, corruption or modification.

- Empower Software Security is used to secure specific areas of the application:
  - Access Rights
    - Functionality
    - Data Sets (Projects)
  - Audit Entries
  - Password Security
  - Sign Off Privileges

- This makes it the easiest CDS to run in a compliant way!!

  (exception is if customer wants to use LDAP for password authentication)
System Policies
System Policies are labelled designating Waters recommendation for policies that should be invoked for:

a) GxP  
b) Electronic Records  
c) Electronic Signatures

However it is the user interpretation that is important!
Empower User Types

- Empower User Types are used to create custom security for the Empower application
- User Types are associated with each User Account
- There is no limit to the number of User Types
  - One person may have one default user type and be “demoted” in other project areas
- Define User Types AFTER you define the workflow processes
Empower User Types

User Type SuperUser Properties

Management | Methods | Data Acquisition | Privileges

- Acquire Samples
- Edit Sample Sets
- Reinject Samples
- Allow Interactive Sys Changes
- Alter Running Sample Sets
- Access Real Time Plot from Open Access
- Alter Any Queue
- Alter My Queue
- Warn On Service Limit
- Use Wizard Templates
- Allow Remote LAC/E Reboot
Empower User Accounts

- Assigns username, password and user types to each User Account

- Each active/disabled Empower user account requires an Empower license
  - removed Empower user accounts do not use a license
  - Can have multiple user type for one user account

- Sharing of user accounts is not permitted
  - By the software licensing regulation (Oracle fined Apotex $1mil)
  - By the FDA

- Audit trails in Empower rely on identification of each user accessing the software.
  - Audit trails are useless if people share a common account
  - Equivalent to forging a signature on a GMP document
System policies governing

User Accounts
User Passwords
Login behavior
User Interface access
### Limited Entry Attempts

#### Configuration Manager

<table>
<thead>
<tr>
<th>Action</th>
<th>User</th>
<th>Change Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified User</td>
<td>longden</td>
<td>12 July 2002 10:19</td>
<td>User: hallam Modified User Status: Disabled -&gt; Active</td>
</tr>
<tr>
<td>Modified User</td>
<td>longden</td>
<td>12 July 2002 10:19</td>
<td>User: hallam Modified User Password Reason: Reactivate</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 10:16</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 10:15</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 10:15</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 10:15</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 09:32</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Auto Purged Message</td>
<td></td>
<td>12 July 2002 09:31</td>
<td>View: Processing</td>
</tr>
<tr>
<td>Auto Purged Message</td>
<td></td>
<td>12 July 2002 09:31</td>
<td>View: Security</td>
</tr>
<tr>
<td>Auto Purged Message</td>
<td></td>
<td>12 July 2002 09:31</td>
<td>View: General</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>longden</td>
<td>12 July 2002 09:31</td>
<td>User: longden Node: Cutting</td>
</tr>
<tr>
<td>Unsuccessful Logon A</td>
<td>longden</td>
<td>12 July 2002 09:31</td>
<td>User: longden Node: Cutting - Incorrect password</td>
</tr>
<tr>
<td>Successfully Logged In</td>
<td>cutting</td>
<td>11 July 2002 18:42</td>
<td>User: cutting Node: Cutting</td>
</tr>
</tbody>
</table>
Empower Projects are folders used to organize chromatographic studies

Establish Name Convention
- Customer Name, Assay Name, Compound, System Name, Analyst Name

User groups are used to design access to different projects
- Separates one labs work from another
Empower Audit Trails ID numbers

- Empower is built into an Oracle Database
- This database gives each object or result a Unique Identifier for tracking the values and records
- This identifier is unique within each project.
- Modification of any database object results in a NEW record with NEW identifiers

- Many users of Empower use these ID number to prove and identify results to auditors
  - Also to track for their own purposes
Assigns Unique ID # for All Entries

<table>
<thead>
<tr>
<th>SampleName</th>
<th>Vial</th>
<th>Sample Set Id</th>
<th>Vial Id</th>
<th>Injection Id</th>
<th>Channel Id</th>
<th>Result Id</th>
<th>Calibration Id</th>
<th>Result Set Id</th>
<th>Processing Method Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>PQ Unk. 4</td>
<td>7</td>
<td>1007</td>
<td>1048</td>
<td>1049</td>
<td>1050</td>
<td>1051</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Unk. 3</td>
<td>6</td>
<td>1007</td>
<td>1044</td>
<td>1045</td>
<td>1046</td>
<td>1047</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Unk. 2</td>
<td>5</td>
<td>1007</td>
<td>1040</td>
<td>1041</td>
<td>1042</td>
<td>1043</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Unk. 1</td>
<td>4</td>
<td>1007</td>
<td>1036</td>
<td>1037</td>
<td>1038</td>
<td>1039</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Std 10x</td>
<td>3</td>
<td>1007</td>
<td>1031</td>
<td>1033</td>
<td>1034</td>
<td>1035</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Std 5.0x</td>
<td>2</td>
<td>1007</td>
<td>1026</td>
<td>1028</td>
<td>1029</td>
<td>1030</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
<tr>
<td>PQ Std 2.5x</td>
<td>1</td>
<td>1007</td>
<td>1004</td>
<td>1009</td>
<td>1010</td>
<td>1017</td>
<td>1012</td>
<td>1011</td>
<td>1000</td>
</tr>
</tbody>
</table>
## Method ID, Version and ‘Locked’

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Date</th>
<th>Method Version</th>
<th>Method Id</th>
<th>Locked</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Alliance</td>
<td>Instrument</td>
<td>15 May 2002 18:48:14</td>
<td>1</td>
<td>1019</td>
<td>✔️</td>
</tr>
<tr>
<td>2  LC PQ</td>
<td>Processing</td>
<td>15 May 2002 18:48:14</td>
<td>1</td>
<td>1020</td>
<td>❌</td>
</tr>
<tr>
<td>3  Parahans with small peaks</td>
<td>Processing</td>
<td>15 May 2002 19:28:09</td>
<td>8</td>
<td>1163</td>
<td>❌</td>
</tr>
<tr>
<td>4  Default Individual Report</td>
<td>Report</td>
<td>15 May 2002 19:35:00</td>
<td>8</td>
<td>1164</td>
<td>❌</td>
</tr>
</tbody>
</table>
The built in Empower Database
- Enables every object to be uniquely referenced
- Can never overwrite data
- Can never mistake which data went with which method
- Ensure easy and accurate data review
Traceability - Linking Information to Records

- Original Processing Method
- Original Instrument Method
- Sample Sets
- Standards used for Calibration
- Calibration Curves
- Unchanged Raw Data File
- E-cord information
- LC/GC System Used
- Unique Result
- Product Code/Stage Reagent LIMS ID
- Who Collected
- Who Processed
- Who Reviewed
- Who Approved
- When
- Why

©2011 Waters Corporation
Built in Audit Trails in Empower

- All user actions are logged in various audit trails and associated with the logged in USERNAME
  - Assumes all users have unique User Account
- It is not possible to create, manipulate, modify or delete data inside Empower without creating an audit trail entry
- Multiple “modes” of audit trail
  - Silent
  - Full – Includes the requirement to enter a reason “Why?”
    - With free form reasons
    - With predefined reasons only
  - Reauthentication (re entry of password to confirm identity)
- Empower Audit trails are not editable or modifiable by ANY USER
Empower Audit Trails

- **Sample Audit Trail**
  - Tracks changes to entered data about each sample

- **Result Audit Trail**
  - Links results to instruments, sample sets, methods, calibration curves and standards used in calibration.
  - Also traces any manual manipulation of data

- **Method Audit Trail**
  - Keeps all versions of method for recreation of results
  - Audit Trail monitors each change, before and after values, who when and why
  - Different versions can be compared to identify the differences
Empower Audit Trails

- **Project Audit Trail**
  - Gives overview of all changes in a project
  - Includes details of method / data deletion

- **System Audit Trail**
  - Shows changes to system objects and system policies
  - Details archive activity
  - Notes all changes to security (users, user types etc)
  - Documents all successful and unsuccessful logins
    - You have a history of who was logged into the application at any time
    - You have information about system break in attempts
    - Includes the client the login/login attempt occurred at
Empower Sample Audit Trail

Sample History


4. Modified Vial(SampleWeight): 1.00000 -> 23.40000
Removing Non Compliant solutions

- The fully feature rich chromatographic application
  - Do all chromatographic calculations inside
  - Built in calculation options
    - System suitability
    - Dissolution
    - GPC
  - Adapt calculations in a compliant way
Inspectors want to see that you have implemented the controls that Empower provides for you

- Unique Usernames for audit trails
- Default strings for reasons WHY you change objects
- Password expiry and history
- Limited access to delete objects in the database

Outside Empower procedures are as important

- Training
- Daily Backup of data