The iCE3 – GMP Ready Out of the Box
A Guide to the iCE3 Software's Key 21 CFR Part 11 Technical Controls

Susan Darling, Humphrey Li, ProteinSimple, 27 Coronet Road, Toronto, ON, Canada M8Z 2L8
Chantal Felten, Alpine Analytical Academy, Whistler, BC, Canada V0N 1B7

Introduction

Electronic data authenticity and integrity are an integral part of GMP manufacturing. The FDA guidance 21 CFR Part 11 defines the characteristics required for GMP compliant electronic records and signatures.

It is important to note that 21 CFR Part 11 compliance specifies additional procedural controls (i.e. notification, training, SOPs, and administration) to be put in place by the user in addition to the technical controls that the software provides. iCE Software contains the following 21 CFR Part 11 technical controls:

- User Log-In Function limits system access to authorized individuals
- Electronic Signature is required throughout run execution, processing and exporting
- A secure, computer generated, time stamped audit trail records the date and time of operator entries and actions that create, modify, or delete electronic records
- The software provides accurate and complete copies of records in both printed and electronic format.
  Note: All iCE software designs are and will remain backwards compatible
- Uses operational system and network domain features to ensure data authenticity and integrity are maintained

  The software uses file string encryption and applies the industry standard checksum algorithm to verify data integrity.

  In addition, in QC-function, operational restrictions strengthen GMP compliant batch execution. For example, once started, a batch may not be modified – the batch must be stopped/aborted, then renamed and restarted. The batch may not be paused and modified.

Content

The focus of this poster is the main 21 CFR Part 11 characteristics embedded in the batch execution function, audit trail and electronic signatures. Also, covered in greater detail are the data processing and data export function which are unique to the iCE system.

Due to the nature of iCE technology, common third party chromatographic software cannot directly receive the IEF data trace. The iCE system performs whole column imaging and generates data in pixels which is very different from a traditional HPLC or CE time-based detection. In order to fit the requirements of the third party software, the data file is processed followed by export to a quantitation software.

Electronic Signatures

All iCE software users must be a Windows local or domain user. User Log-In Authority is defined by the End User.

The system differentiates three types of users:

1. Administrator: Full Access
2. Scientist: Execute /Process/ Review /Export
3. Operator: Execute /Review (QC function only)

- The iCE software e-signature is characterized as a unique identification code and password
  Note: The password expiration is defined by End User IT policy
- When several signings are performed during a continuous session, the password must be entered at each signing
- The iCE software will lock the user account after 3 repeated invalid login attempts and records this event into the audit logs

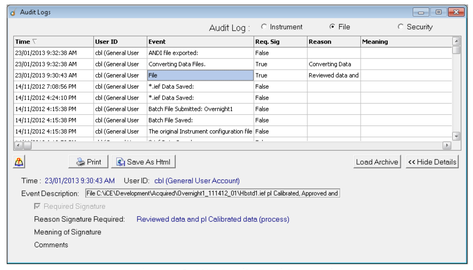

Figure 1: iCE Audit Trail Example

The Audit Trail

The software generates automated secure, time and date-stamped audit trails for the following actions:

1. Instrument: Records all changes to the system configuration including the Instrument Set-Up such as Cartridge Calibration or Tray Type Change.

2. File: Contains audit entries for changes or creation of files such as Sample Processing or Batch Table creation. For each injection ID, the audit trail records **all events** from batch initiation to export of data to third party software.

3. Security: Contains audit entries for User administration of program, such as the User Log-In Audit Trail.

All Audit trails are secure and cannot be altered by the operator. The audit trail detail contains: date/time stamp, operator, event, e-signature requirement, reason/comment description (when applicable).

Raw Data Processing

Requires Electronic Signature

Raw IEF data is processed to create a processed file to support data analysis. In addition to the information securely embedded in the original RAW- IEF file, the pI calibrated data file also includes secure information on processing such as time, date, operator and processing details.

SOFTWARE SAFETY FUNCTION: The RAW-IEF data will be locked once data processing is confirmed in the Batch Review function. For any secondary processing, the IEF file must first be **unlocked** before the file can be reprocessed and the system will overwrite the initial processed file. This process requires an e-signature.

Data Export to Third Party Quantitation Software

Export Processed Data File

Requires Electronic Signature

Processed IEF data are converted to ANDI (Analytical Data Interchange) format for export to a third party chromatographic analysis software such as Chrom Perfect, Empower, or Chromeleon. The ANDI file format supports export of the data trace **embedded with the secure sample specific information**. The amount of sample specific info embedded in the ANDI file is dependent on the conversion method for the specific third party software. For example, due to differences in data files and formats, the conversion to Empower vs. the conversion to Chrom Perfect may contain different amounts of information.

At minimum the ANDI file will contain the following embedded secure sample information: Injection date/time, Sample date/time, system configuration and operator.

Import to 3rd party software

Import of the file and subsequent audit trail is defined by the End User IT system. The amount of embedded sample detail visible after import depends on the third party software.

As shown in the example for Empower, injection date/time, sample date/time, system configuration and operator detail are securely imported to Empower.

Additional information may be added to the resulting Empower injection file by defining a custom import field which can be populated upon import by the analyst.

Example: Empower Import

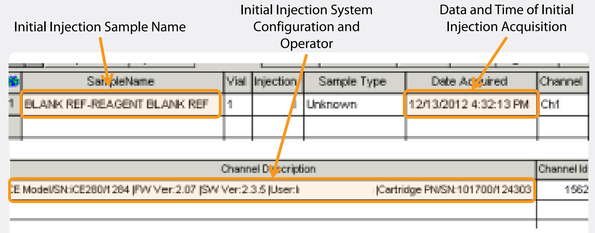

Figure 2: Imported Sample information as shown in Empower 2

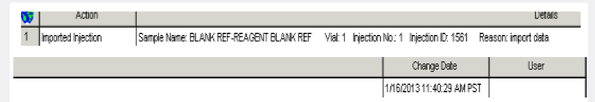

Figure 3: Audit trail as shown in Empower 2 after import

Conclusion

Direct data acquisition in third party chromatographic software is not feasible due to the nature of detection (whole capillary imaging); but the 21 CFR Part 11 compliant process of export and import contained within iCE software allows the End User to transfer the iCE data file securely to a third party software of their choice (i.e. Chromeleon, Empower, or Chrom Perfect).

The iCE software offers all the characteristics required for 21 CFR Part 11 compliance, including:

- Restricted access
- Controlled sequence of events (with secure Audit Trail and e- signatures)
- Data archiving and retrieval capabilities
- Operational restrictions to ensure data authenticity and integrity

The iCE Software has been validated in accordance with ProteinSimple software validation guidelines to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. A validation summary report is available upon request.

In closing, that although iCE software provides the necessary controls for 21 CFR Part 11 compliance, it will still require action on the End User's part to ensure GMP compliant record keeping. For example, End User may consider including instructions in SOP:

- for data archiving to a secure location
- for printing of information that they may choose not to archive electronically (examples include Batch Sequence records and Method detail (time/date stamped)