Biotage® Extrahera™ GLP Software and 21 CFR Part 11 Regulations

Technical Information

The Biotage® Extrahera™ System – Instrument and GLP Software is designed to automate sample preparation in many applications that utilize Solid Phase Extraction (SPE), Supported Liquid Extraction (SLE), Dual Mode Extraction (DME), Phospholipid Depletion (PLD), Protein Precipitation (PPT) and Filtration techniques.

An increasing number of laboratories are using electronic records (ER) and electronic signatures (ES) for exchanging and storing data. Electronic documentation offers many benefits, including increased efficiency and productivity when storing data and easier information sharing and data mining. If a company or laboratory intends to use an electronic format instead of paper for records that are required under FDA regulations and requirements, the company or laboratory must comply with the regulations issued by the FDA: Final Rule 21 CFR Part 11 Electronic Records.

Figure 1. The Biotage® Extrahera™ System with GLP Software.

The Extrahera™ is a closed system, where access is controlled by users who are responsible for the content of the electronic records on that system. The software forms part of the ER system by which electronic records are created, modified, stored and secured against further modification. The Extrahera™ does not provide electronic signature functionality.

The Extrahera™ files shown in Table 1 are electronic records that are affected by 21 CFR Part 11. Compliance of files generated by other software is the responsibility of the ER/ES system operator.

Compliance with 21 CFR Part 11 involves both technical (i.e. hardware and software) and procedural requirements. This Technical Information explains how the Extrahera™ system contributes to fulfilling the technical requirements of 21 CFR Part 11.10: Controls for closed systems.

Examples of the procedural requirement of 21 CFR Part 11.10 that must also be fulfilled include the training of users, the control of system documentation and the control of system access. Fulfilling procedural requirements involves the establishment of standard operating procedures (SOPs) which must be followed by users of the Extrahera™ system. Depending on the specific requirements to be fulfilled, compliance is the responsibility of the company or laboratory operating the Extrahera™, Biotage or both parties. The sections of 21 CFR Part 11.10 and how the Extrahera™, as a closed system, contributes to compliance with them are as follows.

Files	Description
Methods (exported to .exp)	The .exp file is generated when a method is exported. It contains all parameters for a single method including Solvents, Sample Types, Extraction Media, Sample Plates & Racks and Pipette Tips.
Sample Batch Worklist (imported as .xlsx)	The SBWL file allows a user to enter sample details onto the system. The file allows for 12 fields of data entry per sample to be entered (2 are hardcoded) into the system. This data is captured in the report and once uploaded is uneditable. Its primary use is to import the details of a batch of samples to be processed from a LIMS.
Reports (exported to .pdf)	The pdf report file is generated at the end of each run. The user can configure the report parameters to include or exclude various fields. The selected report parameters are tied to a method. The file contains comprehensive data from the method performed (e.g. samples, reagents, setup etc.).
Operational Audit Trail (exported to .pdf or txt)	Logs run data. Each run has its own audit trail that contains more detailed information than the report that is generated at the end of the run. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Methods Audit Trail (exported to .pdf or txt)	Logs all changes to a method. Each method has its own audit trail. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Data Administration Audit Trail (exported to .pdf or txt)	Logs all creations and deletions of custom solvents, sample types, plates, racks, and pipette tips, and locking and unlocking of solvents. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
System Administration Audit Trail (exported to .pdf or txt)	Logs all logins and logouts to the system and actions performed in the System Administration view. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Maintenance Audit Trail (exported to .pdf or txt)	Logs all changes and actions performed in the Maintenance view. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Master Audit Trail (exported to .pdf or txt)	Logs all backup, restore database, import, export, and delete actions performed on the system, and all downloads of reports from the remote viewer. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Service Audit Trail (exported to .pdf or txt)	Logs all changes and actions performed in the Service view. Exported either as a PDF or plain text file. The PDF file is locked using an automatically generated, non-recoverable password and cannot be edited.
Backup (exported to .zip)	The backup file creates an export zip file containing an entire copy of the system database, audit trails and reports.

Table 1. Files that are affected by 21 CFR Part 11

Controls for Closed Systems – 21 CFR Part 11.10

Validation – 21 CFR Part 11.10 (a)

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

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. Such procedures and controls shall include:

This defines the need for validation of the electronic record system installed at the company or laboratory operating the Extrahera™ system.

The Extrahera™ system provides mechanisms to check the validity of electronic records. The electronic records are prepared to enable unauthorized alterations to be detected. The software performs a check when methods are loaded. The software presents a warning when a modified method is loaded.

The company or laboratory must validate the Extrahera™ system as part of the electronic record system.

Readability – 21 CFR Part 11.10 (b)

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.

In table 1 listed are the files that are created or used by the Extrahera™ system. These files are .pdf .txt .zip .xlsx or .exp files that can be viewed and printed via many text or word-processing programs.

Archived record protection – 21 CFR Part 11.10 (c)

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

The software generates a report file in PDF format. The operational audit trail contains more detailed information than the report. The operational audit trail output file can be provided in .txt format for electronic data processing. The Extrahera™ system generates electronic records that do not expire and stay on the file system until the user transfers these files to an external electronic archive. The transfer to an external electronic archive and the management of the electronic archive is under the responsibility and control of the company or laboratory. In addition, the Extrahera™ system issues a warning when remaining disk space is limited but does not delete electronic records.

System security – 21 CFR Part 11.10 (d)

Limit system access to authorized individuals.

User management on the Extrahera™ system enables creation of user accounts based on roles. Access to the system is controlled by user login. Extrahera™ users with “Routine” access can only run methods, view some audit trails and perform limited maintenance, whereas users with “Power” access can manage method settings, manage data admin settings, access the audit trails and execute special maintenance tasks. A user with “Admin” access can manage user accounts and set/amend system parameters but can’t run a method, table 2 shows user privilege permissions in detail. All changes and interactions to the Extrahera are logged in the audit trails.

Audit trail – 21 CFR Part 11.10 (e)

Use of secure, 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 shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Extrahera™ system automatically creates audit trails that record the type of action, the user identification and the date and time of any actions that create or modify the configuration of the system. The audit trails are permanently stored in the database and do not expire. The audit trail information can be exported to a PDF format. The audit trail database repository is protected by the database authorization functionality, so content cannot be modified by the user.

The export of the audit trails with sufficient frequency and the archiving of audit trail data are under the responsibility and control of the company or laboratory.

Sequencing – 21 CFR Part 11.10 (f)

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

The Extrahera™ system performs checks to ensure that users run method files correctly. The user is guided through predefined workflows with step-by step instructions. The system checks and validates the user input on the User Interface (UI). The user must confirm that he or she has followed the worktable setup instruction before initiating a run. All input data is checked again before the system starts an experiment.

Authority – 21 CFR Part 11.10 (g)

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.

Access to software functions is based on a set of permissions. These permissions are related to different user roles. Only authorized users can create, import, export, edit, and lock method, setup and start runs, change software settings or create additional user accounts. It is the responsibility of the company or laboratory to assign the appropriate user role to each individual depending on the desired level of authorization.

Reports and audit trail exported in PDF format are protected against modifications by using default security capabilities of the portable document format. The user is not able to modify the PDF files after they have been created. In addition, method files once validated are protected by locking to prevent inappropriate modification. Once locked the file can only be unlocked by the same user that locked it preventing any changes.

The contents of unlocked method files are audited by the Extrahera™ system. Any modifications to the contents of the file, are recorded and the method cannot be saved unless a reason for change and the power user making said change enters their password. The Extrahera™ system does not provide electronic signature functionality.

Location checks – 21 CFR Part 11.10 (h)

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The validity of the source of data for method files is ensured by protecting it in the Data Administration database. This labware and liquid data is stored and protected in the Data Administration database. This ensures that all input data of a method and consequently a run (except sample ID definition and necessary parametrization) has been generated by authorised personnel or software and that the data have not been altered after generation.

Education/training – 21 CFR Part 11.10 (i)

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Biotage supplies training with the initial installation of the Extrahera™ instrument, and also provides additional trainings on request. In addition, user manuals and documentation are provided by Biotage. Establishing and maintaining the appropriate training level for Extrahera™ users is the responsibility of the company or laboratory. The Extrahera™ system supports fulfilment of this requirement by applying a role-based user management. The Extrahera™ system does not provide electronic signature functionality.

Written policies – 21 CFR Part 11.10 (j)

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

The company or laboratory operating the Extrahera™ system is responsible for establishing the policies and procedures to support compliance with this regulation.

System documentation – 21 CFR Part 11.10 (k)

Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

The Extrahera™ system is delivered together with printed user documentation that is associated with the specific version of the software. The manuals can be downloaded electronically from www.biotage.com The distribution of the documentation to users of the Extrahera™ system and version control of the documentation is the responsibility of the company or laboratory.

Feature	Routine	Power	QA/QC	Admin.	Monitor	Service	Comment
Login to the System	✓(1)	✓(1)	✓(1)	✓	✗	✓	(1) Overridable by a power user when the screen is locked.
Run Methods							
Locked Methods	✓	✓	✗	✗	✗	✗	
Unlocked Methods	✗	✓	✗	✗	✗	✗	
Biotage Methods	✗	✓	✗	✗	✗	✗	
Get E-mail Notifications	✓	✓	✗	✗	✓	✗	
Reports							
Delete	✗	✓	✗	✗	✗	✗	If the reports are only saved in a network share folder, the **Reports** view is disabled to all users.
View and Export as PDF	✓	✓	✓	✗	✗	✗	
Manage Methods							
Create, Import, Export, Edit, and Lock	✗	✓	✗	✗	✗	✗	A method can only be unlocked by the same user that locked it.
View and Export as PDF	✓	✓	✓	✗	✗	✗	
Data Administration							
Create and Delete Entry, and Lock Solvent	✗	✓	✗	✗	✗	✗	Solvents, sample types, extraction media, sample plate and racks, and pipette tips.
View Entry	✗	✓	✓	✗	✗	✗	
System Administration							
Configure Pipette Pump Notifications	✗	✗	✗	✓	✗	✓	
Enable the Remote Viewer	✗	✗	✗	✓	✗	✓	
Manage User Accounts	✗	✗	✗	✓	✗	✓	
Set Date and Time	✗	✗	✗	✓	✗	✗	
Network Services	✗	✗	✗	✓	✗	✗	
Perform and Schedule Backup	✗	✗	✗	✓	✗	✗	
Export Options	✗	✗	✗	✓	✗	✗	
Maintenance							
System Settings	✓	✓	✓	✗	✗	✗	System settings: alarm, lights, instrument type, PPT/PLD mode, and headers for SBWL.
Calibrate Pipette Pump	✗	✓	✓	✗	✗	✗	
Manual Control	✓	✓	✗	✗	✗	✗	
Flush Solvent Inlets	✓	✓	✗	✗	✗	✗	
Export Logs	✓	✓	✗	✗	✗	✗	
Re-initilize the System	✓	✓	✗	✗	✗	✗	
View and Export Audit Trails							
Operational	✓	✓	✓	✗	✗	✗	If the reports are only saved in a network share folder, the operational audit trails are not accessible on the system.
Methods	✓	✓	✓	✗	✗	✗	
Data Administration	✗	✓	✓	✗	✗	✗	
System Administration	✗	✗	✗	✓	✗	✓	
Maintenance	✓	✓	✓	✗	✗	✗	
Master	✗	✗	✗	✓	✗	✓	
Service	✗	✗	✗	✗	✗	✓	
Access Remote Viewer (if enabled)	✓(2)	✓	✓(2)	✗	✓	✗	(2) When logged in to the system.

Table 2. User Access Permissions

Summary

The sections of 21 CFR Part 11.10, their subjects, and how and by whom the subjects are handled are summarized in Table 3.

Section	Subject	Laboratory/ Company	Biotage	Handled By
11.10 (a)	Validation	✓		Policies of the company or laboratory operating the Extrahera™ system
11.10 (b)	Readability		✓	Existence of electronic records in human readable form that are viewable via many software programs
11.10 (c)	Archived	✓	✓	All electronic records are kept on the file system, until the user transfers them to an external electronic archive
11.10 (d)	System Security	✓	✓	Control of access to the Extrahera™ system through individual authentication
11.10 (e)	Audit Trail	✓	✓	The system tracks changes in audit trails which do not expire. The creation of backups is under the responsibility and control of the company or laboratory
11.10 (f)	Sequencing	✓	✓	The system provides guidance and checks for setting up a method. The user has to confirm the setup and loading of the system
11.10 (g)	Authority		✓	Control of access to the system by individual authentication. User cannot modify electronic records or protocols
11.10 (h)	Location Checks	✓	✓	Configuration and methods are checked by the system. The sample ID input and worktable setup is under the responsibility and control of the company or laboratory
11.10 (i)	Education	✓	✓	Manuals and documentation are provided by Biotage. Establishing and maintaining the appropriate training level is the responsibility of the company or laboratory
11.10 (j)	Written Policies	✓		Establishing and maintaining procedures to comply with this regulation is the responsibility of the company or laboratory
11.10 (k)	System Documentation	✓	✓	Extrahera™ system documentation cannot be changed by the user. The distribution of documentation to the users and version control of the documentation is the responsibility of the company or laboratory

Table 3. Responsibilities of the Company/Laboratory and Biotage.

EUROPE
Main Office: +46 18 565900
Toll Free: +800 18 565710
Fax: +46 18 591922
Order Tel: +46 18 565710
Order Fax: +46 18 565705
order@biotage.com
Support Tel: +46 18 56 59 11
Support Fax: + 46 18 56 57 11
eu-1-pointsupport@biotage.com

NORTH & LATIN AMERICA
Main Office: +1 704 654 4900
Toll Free: +1 800 446 4752
Fax: +1 704 654 4917
Order Tel: +1 704 654 4900
Order Fax: +1 434 296 8217
ordermailbox@biotage.com
Support Tel: +1 800 446 4752
Outside US: +1 704 654 4900
us-1-pointsupport@biotage.com

JAPAN
Tel: +81 3 5627 3123
Fax: +81 3 5627 3121
jp_order@biotage.com
jp-1-pointsupport@biotage.com

CHINA
Tel: +86 21 68162810
Fax: +86 21 68162829
cn_order@biotage.com
cn-1-pointsupport@biotage.com

KOREA
Tel: +82 31 706 8500
Fax: +82 31 706 8510
korea_info@biotage.com
kr-1-pointsupport@biotage.com

INDIA
Tel: +91 22 4005 3712
india@biotage.com

Distributors in other regions
are listed on www.biotage.com

Literature Number: PPS628

Biotage®