WHITE PAPER

PerkinElmer MPS 320 Microwave Digestion System for Laboratories Subject to U.S. FDA 21 CFR Part 11 and EU Annex 11

Introduction

In the pharmaceutical manufacturing field, it is critical that computerized systems comply with the U.S. FDA's 21 CFR Part 11 and EU Annex 11 regulations to ensure data accuracy, integrity and reliability, and sample preparation is no exception.

For pharmaceutical QA/QC testing labs conducting trace-elemental analyses, PerkinElmer's MPS 320™ microwave digestion system delivers the flexibility you need for a variety of applications, while providing both confidence in your results as well as in your compliance to 21 CFR Part 11 and EU Annex 11 regulations. The software of the MPS 320 microwave is designed with extra security features to help the laboratory comply with these regulations.

Benefits of the MPS 320 microwave software include:

- **User Management**: The user management restricts access of the instrument software to authorized personnel only. There are three access levels - "user", "admin" and "sys admin" with defined rights.
- **Password Protection**: Specific user ID and password is required for login. All entries and false entries are notified in the audit trail. The activation and deactivation is managed by the admins. The storage of user data is protected from manipulation and read-out.
- **Audit Trail**: All actions, including entries and changes, are tracked and saved in the audit trail. The audit trails can be retrieved with up to 500 entries shown on one page. The audit trail provides the following:
  - Data security
  - Records of all actions and messages with date and time stamp
  - Record of the user ID with appropriate action
  - Continuously written
  - Existing entries cannot be over written
  - Exportable protected pdf to USB
- **Export**: Export of audit trail, methods, user lists and digestion reports is stored on the USB key as a protected pdf and txt file. The protected pdf is tamper-proof for storage, whereas the txt file is created for visualization in the data record viewer.
- **Electronic Records**: Encrypted electronic records are human readable and printable by Adobe Acrobat Reader. Records are not backward editable.

PerkinElmer®
For the Better

The regulations of 21 CFR Part 11 (Title 21 – Food and Drugs of the Code of Federal Regulations) and EU Annex 11 cover overall system compliance and include administrative, procedural and technical elements. Software alone cannot be compliant without the development and implementation of the other elements. The software of the MPS 320 microwave digestion system provides features that, when coupled with appropriate policies and procedure, fulfill the requirements for closed-system electronic records in 21 CFR Part 11, as well as the elements relating to electronic signatures.

21 CFR Part 11 Requirements vs. Technical Implementation of the MPS 320 Microwave Digestion System

§11.10 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.

Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

The MPS 320 microwave is a closed system. The following table summarizes the requirements of 21 CFR Part 11 for electronic records compared to the technical implementation in the MPS 320:

FDA 21 CFR Part 11 **Subpart B – Electronic Records**				
Reference	**Term**	**PerkinElmer Responsibility**	**User Responsibility**	**MPS 320 Solution**
Controls for Closed Systems				
§11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Performance tests and validations are done before the release of a new product in accordance with the internal quality regulations and ISO 9001. - Quality management in place (change management, development process) - ISO certification - Qualification package available	- Assure correct installation and functionality of the instrument - Perform instrument qualification on a regular basis - Instrument is working as expected and functioning - Preventive maintenance is performed - PQ tests	- DIN EN ISO 9001 - IQ/OQ package - Repeating OQ - The IQ/OQ service is available and ensures correct installation (IQ) and functionality (OQ) as specified by PerkinElmer - Templates and guidelines for preventive maintenance
(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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	- Technical conditions of the instrument to generate audit trail and export and print functionality - Provide file exports and generate printable reports - Export function for methods, digestions, user lists and audit trail in an unchangeable file format	- Export of reports on a regular basis	- All data is stored on the controller of the MPS 320 and can be printed and exported as pdf and txt files - Audit trail is automatically generated - Data export function contains user and time stamp

FDA 21 CFR Part 11 Subpart B – Electronic Records				
Reference	**Term**	**PerkinElmer Responsibility**	**User Responsibility**	**MPS 320 Solution**
Controls for Closed Systems				
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Access control to instrument functionality and information. Users can be created by an admin within the defined administration levels. The admin defines an initial password, which must be changed by the user, at the next login. **User management:** - Individual user IDs - User levels **Password protection:** - Password expiration - Password security level - User locked after 5 false entries Tracked in audit trail	- Backup of data on a regular basis - Archiving of the exported data on an appropriate medium - Install corresponding reading tool on the relevant PC	- User management with access control by user administration (user ID/ password) - Password protection - Password security/ complexity rules - User identification (ID, first name, last name) - Password expiration (60 days) - Locking after 5 false entries – activation by admin required - Users are able to change the password at any time
(d)	Limiting system access to authorized individuals.			
(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.	Audit trail is continuously written and exportable as pdf It contains: - One entry per action - Date and time stamp - Numbering of entries - Serial number - User	- Export of reports on a regular basis to a suitable media	- Audit trail entry per activity with time and ID stamp - Audit trail entries are not accessible for alteration - The audit trail can be exported as pdf for storage and as csv for easy sorting and filtering
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	- Preinstalled factory methods - Error messages - Warning messages	- Instructions must be entered in an SOP	- Predefined steps in applications and methods - Error and warning messages

FDA 21 CFR Part 11 Subpart B – Electronic Records				
Reference	**Term**	**PerkinElmer Responsibility**	**User Responsibility**	**MPS 320 Solution**
Controls for Closed Systems				
(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 control - User management - Audit trail entries	- Definition and control of authorized users	- Software access control (user ID / password) according to the rights of the account
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	- Hardware is identified via serial number, to ensure that only valid configurations are in use		- Serial number and coding to control allowed device combinations - Listed in the audit trail in the startup information
(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.	- PerkinElmer assists individual customer, distributor and service engineers training	Define responsibilities and implement them in the defined level as user, admin or system admin - Internal trainings to qualify users - Read the operation manual - Regular instrument qualification (OQ) - Preventive instrument maintenance	
(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.	- PerkinElmer provides hardware and software manuals, updated per release, and delivered with product - Change history in all documents - The PerkinElmer quality management assures that hardware and software is tested and revised before the release	- Storage of the documentation - Provide each user access to operation manual - Change and configuration management	- Change history listed in the documents - Operation manuals are delivered with the instrument - The documentation contains change history and versioning - IQ/OQ services for qualification

FDA 21 CFR Part 11 Subpart B – Electronic Records				
Reference	**Term**	**PerkinElmer Responsibility**	**User Responsibility**	**MPS 320 Solution**
Signature Manifestations				
§11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature		- Definition of user level as specified	- Time stamped audit trails identify the corresponding user and contain date, time, name and meaning
(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).	- Export and printout of reports		- This information is also contained on report views and printouts
Signature/Record Linking				
§11.70	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.	- Records cannot be changed - Entry in the audit trail of each activity includes user ID with details of the user		- All user activities are tracked in the audit trail (access control)

FDA 21 CFR Part 11 Subpart C - Electronic Signatures				
Reference	**Term**	**PerkinElmer Responsibility**	**User Responsibility**	**MPS 320 Solution**
General Requirements				
§11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	- Accounts can be activated, deactivated or deleted by the admin - Identical IDs are impossible as the ID is linked to the creation date and time	- Administration of the users by the admin - Passwords must not be provided to third person - Usernames must not be identical to different users - Export and storage of user lists on a regular basis	- User accounts are unique with individual ID, username and password
Controls for Identification Codes / Passwords				
§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). (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.	- Unique combination of user ID, name and password in the software to create an account - Defined validity period of the password - Track of logins and failed login trials in the audit trail - Password hidden during entry	- User can be deactivated by an admin - Protection of the password from the third person	- Password expiration after 60 days - User is locked after 5 false entries and must be reactivated by an admin - Failed logins are recorded and listed in the audit trail - Defined password security level - The new password must be different from the old password

Typical questions about 21 CFR Part 11 compliance of the MPS 320 microwave digestion system software

FAQs	
Question	**Answer**
Is it possible to create individual user accounts?	Yes, user accounts can be created with individual ID and name within the defined user groups.
Is it possible to log out when a digestion is running?	Yes
Is there a password expiration?	Yes, the password expires after 60 days and must be changed.
Will the software be locked after repeated unauthorized attempts?	Yes, after 5 false entries of the ID and password, the user is locked.
How many users can be logged in at the same time?	Only one.
Is there an audit trail to capture all changes and actions?	Yes
Can the audit trail file be modified?	No
Is there an export function to save the records?	Yes, methods, result files, user list and audit trails can be exported to USB.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs

Copyright ©2022, PerkinElmer, Inc. All rights reserved. PerkinElmer® is a registered trademark of PerkinElmer, Inc. All other trademarks are the property of their respective owners.

766800 PKI