Technical Information

QIAcube® HT System and 21 CFR Part 11 Regulations

The QIAcube HT system — instrument and QIAcube HT Prep Manager Software — is designed to perform automated mid- to high-throughput nucleic acid purification in 96-well format in molecular biology applications. In combination with QIAGEN kits indicated for use on the QIAcube HT, the instrument is intended for the applications described in the respective QIAGEN kit handbooks.

Note: The QIAcube HT is intended for molecular biology applications. This product is not intended for the diagnosis, prevention or treatment of a disease. The QIAcube HT is intended for use by professional users trained in molecular biological techniques and the operation of the QIAcube HT.

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*.

The QIAcube HT 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 QIAcube HT does not provide electronic signature functionality.

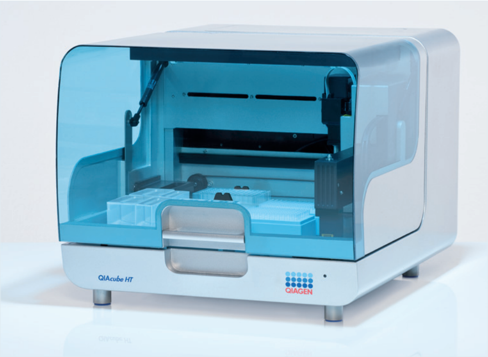

Figure 1. The QIAcube HT System.

The QIAcube HT files shown in Table 1 are electronic records that are affected by 21 CFR Part 11. Compliance of files generated by other software, such as sample files, is the responsibility of the ER/ES system operator.

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

Data set	Description
Kit configuration (.xml)	The kit configuration is a protocol file defined by QIAGEN. The file contains instructions for the experiment procedure and can be parametrized by the user in the experiment setup wizard.
Experiment file (.xml)	The experiment file is the parametrized protocol for a single experiment. The file contains all instructions as well as runtime information.
Report file (.pdf)	The report file is a human readable file in PDF format optimized for printing that the user can opt to create after execution of an experiment. The user can configure the system to indicate whether the software creates a basic or advanced report with fixed structure. The file contains comprehensive data from the automated experiment procedure performed (e.g., samples, output, reagents, setup).
Output file (.xml)	The output labware file in .xml format is optimized for electronic data transfer or computational parsing, and can be created by the user after execution of an experiment. The file contains comprehensive data from the automated experiment procedure performed that describe output labware and its contents.
Audit trail (export to .pdf)	The audit trail is a log of all user interactions that create, modify or delete electronic records. The audit trail is stored in the QIAcube HT system database and can be exported to PDF format.

Compliance with 21 CFR Part 11 involves both technical (i.e. hardware and software) and procedural requirements. This Technical Information explains how the QIAcube HT 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 QIAcube HT system. Depending on the specific requirements to be fulfilled, compliance is the responsibility of the company or laboratory operating the QIAcube HT, QIAGEN or both parties. The sections of 21 CFR Part 11.10 and how the QIAcube HT, as a closed system, contributes to compliance with them are as follows.

Controls for Closed Systems – 21 CFR Part 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. Such procedures and controls shall include:

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.

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

The QIAcube HT 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 checksum validation when such a file is loaded. The software presents an error or a warning when a modified record is loaded.

The company or laboratory must validate the QIAcube HT 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 we listed the files that are created or used by the QIAcube HT system. These files are text or .xml files that can be viewed and printed via many text or word-processing programs.

Protocol files and configuration data are created by QIAGEN personnel only. The software generates a report file in PDF format. An additional output file is provided in .xml format for electronic data processing.

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 QIAcube HT 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 (e.g., by cut and paste) and the management of the electronic archive is under the responsibility and control of the company or laboratory. In addition, the QIAcube HT 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 of the QIAcube HT system enables creation of user accounts based on roles. Access to the system is controlled by user login. QIAcube HT users with “Operator” access can only run protocol files and perform assay setup, whereas users with “Administrator” access can change specific software settings, manage user accounts, access the audit trail and execute special maintenance tasks. All changes to the user database are logged in the audit trail. ▷

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.

The QIAcube HT system automatically creates an audit trail that records 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 trail is permanently stored in the database and does not expire. The audit trail information can be queried and restricted to the desired contents (e.g., based on date and time information, special users) before export 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 creation of exports from the audit trail database 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 QIAcube HT system performs checks to ensure that users run protocol files correctly. Only protocols provided by QIAGEN can be run on the system. 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 an experiment. 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 add or delete files, setup and start experiments, 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.

The content of experiment files is signed with a signature by the QIAcube HT system. Any modification to the content of the file, including the signature itself, invalidates the experiment file.

Reports and audit trail exports 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, configuration files, protocol files and electronic readable result files are protected by using a checksum to detect inappropriate modification. The checksum is an alpha-numerical value assigned to a file by the system and is based on the content of the file. The file is invalid if the checksum does not match the file's content or if it is missing. The QIAcube HT system will show an error indicating an invalid checksum when the user tries to load an invalid .xml file.

The QIAcube HT 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 configuration data and protocol files is ensured by validating the checksum of the files. The labware data is stored and protected in the database. This ensures that all input data of an experiment (except sample ID definition and necessary parametrization) has been generated by QIAGEN 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.

QIAGEN supplies training with the initial installation of the QIAcube HT instrument, and also provides additional trainings on request. In addition, user manuals and documentation are provided by QIAGEN. Establishing and maintaining the appropriate training level for QIAcube HT users is the responsibility of the company or laboratory. The QIAcube HT system supports fulfillment of this requirement by applying a role-based user management. The QIAcube HT 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 QIAcube HT 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 QIAcube HT system is delivered together with electronic user documentation that is associated with the specific version of the software. The manuals are provided in PDF as well as online help and cannot be changed by the user. The electronic user manual is installed with the software and can easily be reached via the help menu or icons.

The distribution of the documentation to users of the QIAcube HT system and version control of the documentation is the responsibility of the company or laboratory.

Summary

The sections of 21 CFR Part 11.10, their subjects, and how and by whom the subjects are handled are summarized in Table 2.

Table 2. Responsibilities of the Company/Laboratory and QIAGEN

Section	Subject	Laboratory/ Company	QIAGEN	Handled by
11.10 (a)	Validation	✓		Policies of the company or laboratory operating the QIAcube HT 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 QIAcube HT system through individual authentication
11.10 (e)	Audit trail	✓	✓	The system tracks changes in an audit trail which does 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 an experiment. Only QIAGEN protocols can be run. The user has to confirm the setup and loading of the worktable
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 protocols 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 QIAGEN. 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	✓	✓	QIAcube HT 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

For up-to-date licensing information and product-specific disclaimers, see the respective QIAGEN kit handbook or user manual. QIAGEN kit handbooks and user manuals are available at **www.qiagen.com** or can be requested from QIAGEN Technical Services or your local distributor.