Technical Information

The QIAcube® Connect System and 21 CFR Part 11 Regulations

The QIAcube Connect system — QIAcube Connect and its operating software — is designed to perform automated nucleic acid purification of QIAGEN´s spin column kits indicated for use on the QIAcube Connect instrument. In combination with the QIAsphere Base Gateway (Q-Base) and the QIAcube Connect App, the QIAcube Connect instrument allows its users to stay connected, monitor runs remotely, and thus enables quick response times (Figure 1).

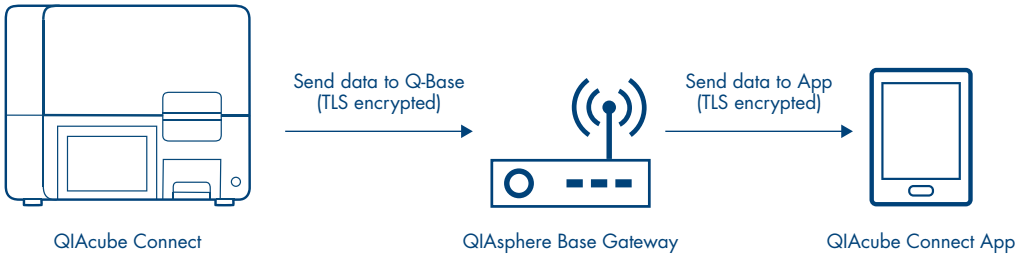

Figure 1. QIAcube Connect architecture diagram. The communication from the instrument to the app is supported unidirectional via the QIAsphere Base Gateway.

An increasing number of laboratories are using electronic records and electronic signatures 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.

QIAcube Connect 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 electronic record system by which electronic records are created, modified, stored and secured against further modification. QIAcube Connect does not provide electronic signature functionality.

Compliance with 21 CFR Part 11 involves both technical (i.e., hardware and software) and procedural requirements. In this Technical Information we explain how the QIAcube Connect system, referred to as "the system" below, complies with the technical requirements of the FDA, hereinafter referred to as "the agency", under regulation 21 CFR Part 11.10: *Controls for closed systems*.

Examples of the procedural requirement of 21 CFR Part 11.10 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 system. ▷

Depending on the specific requirements to be fulfilled, compliance is the responsibility of the company or laboratory operating the QIAcube Connect, QIAGEN or both parties. The sections of 21 CFR Part 11.10 and how QIAcube Connect, as a closed system, contributes to compliance with these sections are as follows.

Controls for Closed Systems – 21 CFR Part 11.10

The sections of 21 CFR Part 11.10 are listed in Table 1 together with the respective subject, requirement and description on how the requirement has been implemented.

Table 1. Sections of 21 CFR Part 11.10 and their implementation on the QIAcube Connect system

Section	Subject	Requirement	System implementation
11.10 (a)	System validation	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The QIAcube Connect Operating Software is validated by QIAGEN to ensure accurate, reliable and intended performance of the QIAcube Connect system. IQ/OQ procedures for the proper function of the instrument can be put in place. The software performs a checksum validation to check the validity of electronic records.
11.10 (b)	Record generation	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.	The QIAcube Connect operating software generates run-specific report files in a human-readable form (PDF format). An additional output file is provided in XML format for electronic data processing.
11.10 (c)	Record protection	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The QIAcube Connect 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. Security measures for report storage outside of the system lie within the responsibility of the operating company or laboratory. In addition, the QIAcube Connect system issues a warning when remaining disk space is limited, but it does not delete electronic records.
11.10 (d)	Access limitation	Limiting system access to authorized individuals.	Access to the system is controlled by user login. User management of the QIAcube Connect system enables creation of user accounts based on roles. Users with "Operator" access can select and run protocol files, download report files and execute instrument maintenance protocols. In addition to that, users with "Administrator" access can change time, date and network settings, add or delete protocol files, update the operating software, manage user accounts, access the audit trail and execute special maintenance tasks. All changes to the user database are logged in the audit trail.
11.10 (e)	Audit trails	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.	A time-stamped audit trail records the type of action, the user identification and any action (setup or start of a run, start of a maintenance task). For data protection reasons the users are anonymized in the audit trail – and the user with administrator rights can map an anonymized user to a real user in the user management. The user cannot alter the process-relevant configuration or calibration of the system. The audit trail is stored in the internal file system, which is not accessible by the user. The audit trail contains the last 10,000 entries, which means the history of at least the last 2 years. The audit trail file is circular, meaning that once it is full, it is overwritten from the beginning. Hence, for archiving purposes, a regular download is recommended. The audit trail information cannot be deleted or changed by the user. The audit trail is part of the support package and as such can be downloaded in CSV file format via the support package download functionality. During a software update, the configuration and calibration are kept.

Section	Subject	Requirement	System implementation
11.10 (f)	Operational system checks	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The QIAcube Connect user interface provides a guided step-by-step run setup with user confirmation, and the instrument performs a final worktable load check before executing a protocol run. Only protocols provided by QIAGEN can be run on the system. The user cannot change the sequencing steps that are defined in the protocols.
11.10 (g)	Authority checks	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 the assigned user role (Operator or Administrator). It is the responsibility of the company or laboratory to assign the appropriate user role to each individual user, depending on the desired level of authorization. The QIAcube Connect system does not provide electronic signature functionality.
11.10 (h)	Device checks	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 protocol input or configuration data is ensured by checksum validation by the system. 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. The system software applies checks to allow only valid information input in respective fields.
11.10 (i)	Education and training	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 developers are fully and continuously trained. QIAGEN offers optional training of the QIAcube Connect instrument. A release-specific electronic instrument user manual is distributed together with the software. Establishing and maintaining the appropriate training level for QIAcube Connect users is the responsibility of the company or laboratory. The QIAcube Connect system supports fulfillment of this requirement by applying role-based user management. The QIAcube Connect system does not provide electronic signature functionality.
11.10 (j)	Written policies	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.	Responsibility of the operating company or laboratory. The QIAcube Connect system does not provide electronic signature functionality.
11.10 (k)	System documentation	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.	A release-specific electronic instrument user manual is distributed together with the software. The manuals are provided in PDF and cannot be changed by the user. Within QIAGEN there is revision and change control procedure to maintain the user manual.

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 operating Company/Laboratory and QIAGEN

Section	Subject	Company/Laboratory	QIAGEN	Responsibility handling
11.10 (a)	System validation	x		Policies of the company or laboratory operating the QIAcube Connect system.
11.10 (b)	Record generation		x	Existence of electronic records in human-readable form and exportation to PDF standard.
11.10 (c)	Record protection	x	x	All electronic records are kept on the file system until the user transfers them to an external electronic archive.
11.10 (d)	Access limitation	x	x	Controlled access to the QIAcube Connect system through user authentication. Assigning appropriate user roles lies within the responsibility of the operating company or laboratory.
11.10 (e)	Audit trails	x	x	System tracks changes in an audit trail that does not expire. The creation of backups is under the responsibility and control of the operating company or laboratory.
11.10 (f)	Operational system checks	x	x	Guided run setup with user confirmation and load check of the instrument. Only QIAGEN protocols can be run.
11.10 (g)	Authority checks	x	x	Controlled access to the system by user authentication. User cannot modify electronic records or protocols. Operating company or laboratory has to ensure that each user name can be traced to a real individual and to ensure correct assignment of roles.
11.10 (h)	Device checks	x	x	Checksum validation for configuration and protocols by the system. The sample ID and kit information input, as well as worktable setup, is under the responsibility and control of the operating company or laboratory.
11.10 (i)	Education and training	x	x	Manuals and documentation are provided by QIAGEN. Establishing and maintaining the appropriate training level is the responsibility of the operating company or laboratory.
11.10 (j)	Written policies	x		Establishing and maintaining procedures to comply with this regulation is the responsibility of the operating company or laboratory.
11.10 (k)	System documentation	x	x	QIAcube Connect 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 operating company or laboratory.

QIAcube Connect is designed to perform fully automated purification of nucleic acids and proteins in molecular biology applications. This product is not intended for the diagnosis, prevention or treatment of a disease. The system is intended for use by professional users trained in molecular biological techniques and the operation of QIAcube Connect.