Technical Information

The QIAquant® System and 21 CFR Part 11 Regulations

The QIAquant system — the QIAquant instrument and its operating software — is designed to perform the amplification and quantitative detection of nucleic acids targets in qPCR applications.

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.

According to 21 CFR Part 11, the QIAquant 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. The QIAquant provides electronic signature functionality.

Compliance with 21 CFR Part 11 involves both technical (i.e., hardware and software) and procedural requirements. This Technical Information explains how the QIAquant system, referred to as "the system" in the following, contributes to fulfilling the technical requirements of FDA regulation 21 CFR 11.10: Controls for closed systems.

The QIAquant system is compatible with 21 CFR Part 11 only when used with the desktop version of QIAquant 96 Software and QIAquant 384 Software. The touchscreen version of the software, QIAquant Software Touch, is not fully compatible with 21 CFR Part 11 as it does not encompass user management functionality. The statements in this technical information are only valid for the use of QIAquant instruments in conjunction with the desktop version of QIAquant 96 Software and QIAquant 384 Software.

Figure 1. The QIAquant 96 and QIAquant 384 instruments.

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 system. Depending on the specific requirements to be fulfilled, compliance is the responsibility of the company or laboratory operating the QIAquant instrument, QIAGEN, or both parties. The sections of 21 CFR Part 11.10 and how the QIAquant, as a closed system, contributes to compliance with them 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, description of implementation of the requirement in the system, and the resulting compliance status.

Table 1. Sections of 21 CFR Part 11.10 and their implementation in the QIAquant system

Section	Subject	Requirement	System implementation	Status
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 QIAquant Software is validated by QIAGEN to ensure accurate, reliable and intended performance of the QIAquant instrument. IQ/OQ procedures for the proper function of the instrument can be put in place. The software performs a checksum validation to check the integrity and validity of electronic records.	**Compliant**
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 QIAquant Software generates run-specific report files in a human-readable form (text or PDF format). An additional output file is provided in .qrts and .qrts384 for template files and .qrtp and .qrtp384 for the project files for electronic data processing.	**Compliant**
11.10 (c)	Record protection	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The QIAquant Software 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.	**Compliant**
11.10 (d)	Access limitation	Limiting system access to authorized individuals.	Access to the system is controlled by user login. User management of the QIAquant system enables creation of user accounts based on roles. Users with an "Administrator" role have unlimited rights to all program functions. They can create, delete, edit, lock and unlock users and assign rights to them. Users with "Supervisor" access have the same rights as an administrator, but administrators can block certain rights of supervisors. Users with an "Operator" role can use an existing template but not create a new template or save projects. Any changes to the user database are logged in the audit trail.	**Compliant**
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 user identification, any electronic signatures and recorded actions (for creation or modification to a run template). The Administrator can set which users can see the audit trail and only the username of the user will be displayed (not the full name). The user cannot alter the process-relevant configuration or calibration of the system. The audit trail is stored in the project files and integrity is ensured by checksum verification. During a software update, the configuration and calibration are kept.	**Compliant**

▷

Section	Subject	Requirement	System implementation	Status
11.10 (f)	Operational system checks	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The QIAquant Software user interface provides a guided step-by-step run setup. Only parameters within the acceptable range of the system can be selected and set to ensure that the system runs within specifications at any time.	**Compliant**
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, Supervisor 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 QIAquant system provides electronic signature functionality for templates and projects. The user roles can be adjusted to allow the authority to sign or not (by the Administrator).	**Compliant**
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.	**Compliant**
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 or contracted developers are fully and continuously trained. All software undergoes a documented software release process before being made available to users. Establishing and maintaining the appropriate training level for QIAquant users is the responsibility of the company or laboratory. The QIAquant system supports fulfillment of this requirement by applying role-based user management.	**Compliant**
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.	This is the responsibility of the operating company or laboratory. The QIAquant system supports fulfillment of this requirement by applying a role-based user management and electronic signature functionality. The user roles can be adjusted to allow the authority to sign or not (by the Administrator).	**Compliant**
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 user manual is distributed together with the QIAquant Software. Manuals are provided in printed version and downloadable PDF from the QIAquant webpage and cannot be changed by the user. Within QIAGEN, there is a revision and change control procedure to maintain the user manual.	**Compliant**

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. RResponsibilities 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 QIAquant system.
11.10 (b)	Record generation		x	Existence of electronic records in human readable form and exportable.
11.10 (c)	Record protection	x	x	All saved 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 QIAquant 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 which 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 preventing out-of-specification use of the instrument.
11.10 (g)	Authority checks	x	x	Controlled access to the system by user authentication. Users 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 other information input as well as plate or sample layout 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	QIAquant 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.

The QIAquant system is designed to perform the amplification and quantitative detection of nucleic acids targets in qPCR applications. The system is intended for use by professional users trained in molecular biological techniques and the operation of the QIAquant.