QIAcuity® Digital PCR System and 21 CFR Part 11 Regulations*

The QIAcuity Digital PCR System – instrument, instrument control software (CSW), and QIAcuity Software Suite – is designed to deliver precise and multiplexed quantification results for mutation detection, copy number variation (CNV), gene expression studies, gene-editing analysis, and many more. This nanoplate-based system seamlessly integrates a standard dPCR workflow of partitioning, thermocycling and imaging into a walk-away automated platform with minimal hands-on time.

Note: The QIAcuity is intended for molecular biology applications. This product is not intended for the diagnosis, prevention or treatment of a disease.
Therefore, the performance characteristics of the product for clinical use (i.e., diagnostic, prognostic, therapeutic or blood banking) is unknown.

Electronic records and signatures

An increasing number of laboratories are using electronic records (ER) and electronic signatures (ES) for exchanging and storing data. 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 QIAcuity is a closed system, where access is controlled by users who are responsible for the content of the electronic records on that system. The QIAcuity Software Suite is used to analyze plate results generated at the instrument. Plates are stored in the password protected QIAcuity database and may be used for multiple analysis. All changes are captured by the audit trail functionality of the QIAcuity system. After the analysis of a plate, a report can be created which forms the electronic record. These electronic records are stored within the QIAcuity Software Suite storage space as pdf file. Modification of files within the storage space is protected by Windows® access control mechanism. If required, reports may be signed using the electronic signature functionality of the QIAcuity Software Suite. Exported records need to be secured by the user.

The company or laboratory operating the QIAcuity system need to ensure appropriate permission management of the operating system e.g., granting administrator rights to users should be avoided.

Figure 1. The QIAcuity One, QIAcuity Four, and QIAcuity Eight.

* Valid from QIAcuity Software version 2.1 (Released June 2022)

The QIAcuity 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
Report file (.pdf)	The report file is a human readable file in PDF format optimized for printing that the user can create after execution of an experiment. During the analysis, the user can select which results are used to generate a report and can then select additional elements such as run details, plate general data, plate layout, reaction mix list, and comments. See Table 2 for details of report elements.
Audit trail (export to .pdf)	The audit trail is a log of all user interactions that modify the system by any software interaction and create, modify or delete electronic records. The audit trail is stored in the QIAcuity system database and can be exported to PDF format.

Table 2. Report elements

Data set	Description
Report name	Specific name of the report
Run details	User, Start and end time, Run steps, Run status, Software and Instrument version, dPCR steps
Plate general data	Plate name, type, description, plate owners, labels, barcode
dPCR parameters	Priming profile, Cycling profile (temperature with time duration), Imaging profile (channel, exposure duration, gain)
Plate layout	List of all the elements added to each well
Reaction mixes list	List of all defined reaction mixes with details about each target
Comments	More information/details/descriptions
Result table	Concentration and confidence intervals of results partitions
Signers	Users who signed the report
Date and time	Date and time, including timezone offset

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

This Technical Information also addresses further technical requirements of subpart B, such as 21 CFR Part 11.50: Signature manifestation and 21 CFR Part 11.70: Signature/record linking.

Furthermore, this Technical Information contributes to subpart C (Electronic signature). In particular, 21 CFR Part 11.100: General requirements, 21 CFR Part 11.200: Electronic signature components and controls, and 21 CFR Part 11.300: Controls for identification codes/passwords are explained.

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 the following:

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 QIAcuity system. The QIAcuity is verified by QIAGEN to ensure accurate, reliable and intended performance of the QIAcuity system. IQ/OQ procedures for the proper function of the instrument can be put in place and requested at any time.

These electronic records are stored within the QIAcuity Software suite storage space as pdf file. Modification of files within the storage space is protected by Windows access control mechanism.

Exported records need to be secured by the user. The company or laboratory must validate the QIAcuity 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, files are listed that are created by the QIAcuity system. These files are .pdf files that can be viewed and printed via a pdf reader. Additional output files may be generated in .csv format for electronic data processing.

Archived – 21 CFR Part 11.10 (c)

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

The QIAcuity systems generate electronic records that do not expire and stay within a storage space of the QIAcuity Software Suite. The Windows® access control mechanism protects the modification of files within the storage space. The company or laboratory operating the QIAcuity system is responsible for the Windows access control. They are also responsible for ensuring backups at an appropriate frequency and securing measures for report storage outside the system. In addition, the QIAcuity Suite issues a warning when remaining disk space is limited but does not delete electronic records.

System security – 21 CFR Part 11.10 (d)

Limiting system access to authorized individuals.

Access to the system is controlled by user login. Centralized user management of the QIAcuity system enables creation of user accounts based on roles. Users with "Administrator" access can manage user accounts and execute special maintenance tasks and have access to all other functionalities. All other user roles – Supervisor, Group Leader, Technician, and Quality Assurance for GMP, and Operator for MBA – have limited specific permissions. In addition, as from QIAcuity software version 2.1, new roles can be defined and permissions can be assigned, individually. The user credentials are synchronized with QIAcuity instrument control software using an encrypted communication channel.

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.

An audit trail feature is available and can be controlled by users having the required permissions, such as an administrator. Audit trail will track all changes (events), together with user name and time. The audit trail is permanently stored in the database and does not expire. The audit trail can be accessed by restricted users and 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.

Operational system checks – 21 CFR Part 11.10 (f)

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

Access to the QIAcuity Software Suite requires a login procedure. Furthermore, access to specific plates and reports can be controlled by granting user specific permissions.

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 the assigned user role (Administrator, Supervisor, Group Leader, Technician, and Quality assurance for GMP, Administrator or Operator for MBA), and any other user defined user role. 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 QIAcuity system offers the option to add an electronic signature when a report is created. This electronic signature includes the user name, password, the reason for signing, and the time including timezone offset. Multiple users may sign a report if their permissions allow.

Reports and audit trail exports in pdf format are protected against modifications by using default security capabilities of the portable document format. These files are stored within the QIAcuity Software Suite storage space. Modification of files within the storage space is protected by Windows access control mechanism.

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.

Connection between the QIAcuity Instrument and the Software Suite uses an encrypted communication channel. Any human input is linked to the logged-in user.

Education – 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 developers are fully and continuously trained. QIAGEN offers optional training of the QIAcuity instrument. A release-specific electronic instrument user manual is distributed together with the software. Establishing and maintaining the appropriate training level for QIAcuity users is the responsibility of the company or laboratory. The QIAcuity system supports fulfillment of this requirement by applying a role-based user management.

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 QIAcuity system is responsible for establishing the policies and procedures to support compliance with this regulation. The QIAcuity allows for an electronic signature when a report is created. Multiple users may sign a report if their permissions allow.

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.

A release-specific electronic instrument user manual is distributed together with the software. These user manuals are provided in pdf format and are protected by using

default security capabilities of the portable document format. Within QIAGEN there is a revision and change control procedure to maintain the user manual. The distribution of the documentation to users of the QIAcuity system and version control of the documentation is the responsibility of the company or laboratory.Signature manifestation – 21 CFR Part 11.50

Signature – 21 CFR Part 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.

As from QIAcuity Software version 2.2, the following information is added to a report when a signed report pdf is created:

(1) The printed name of the signer;

(2) The date and time when the signature was executed;

(3) The meaning (reason for a signature).

Record generation – 21 CFR Part 11.50 (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).

The following information entered during the signing process will become part of the report and will be shown on electronic displays or printouts.

(1) The printed name of the signer;

(2) The date and time when the signature was executed;

(3) The meaning (reason for a signature).

Signature/record linking – 21 CFR Part 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.

The QIAcuity system only supports electronic signatures for electronic records (reports) and these are linked to the respective electronic record. Linking to handwritten signatures is not in the scope of the QIAcuity Software Suite and needs to be done by an external document control system.

General requirements – 21 CFR Part 11.100

Uniqueness of eSignature – 21 CFR Part 11.100 (a)

Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

The user name is a unique feature in the user management. Policies of the company or laboratory operating the QIAcuity system need to ensure that each individual uses their own user account.

Verify identity of individuals – 21 CFR Part 11.100 (b)

Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

The company or laboratory operating the QIAcuity system is responsible for establishing the policies and procedures to verify the identity of a user. The user management used in the QIAcuity Software Suite then facilitates the identification of that user by the combination of user name and password. Policies of the company or laboratory operating the QIAcuity system need to ensure that passwords are kept confidential.

Legally binding signatures – 21 CFR Part 11.100 (c)

Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. ▷

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Training of persons using electronic signatures need to be provided on an organizational level. This includes certifications and testimonies.

Electronic signature components and controls – 21 CFR Part 11.200

Non biometric eSignatures – 21 CFR Part 11.200 (a)

Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

An electronic signature as implemented in the QIAcuity Software Suite from version 2.1 onward is the combination of two distinct identification components which are the username and the password. The username and password is needed to access the QIAcuity Software Suite which provides the signing functionality where the password is needed to confirm the electronic signature of the user that is logged in. From version 2.2 onwards, additional validation of the user by entering the user name during report signing is implemented. The company or laboratory operating the QIAcuity system is responsible for establishing the policies and procedures to support compliance with (2) and (3).

Biometric eSignatures – 21 CFR Part 11.200 (b)

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

N/A - Biometric eSignatures are not implemented into the QIAcuity Software.

Controls for identification codes/passwords – 21 CFR Part 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:

Uniqueness of eSignature – 21 CFR Part 11.300 (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.

An electronic signature as implemented in the QIAcuity Software Suite from version 2.1 onward is the combination of a user name and a password which is controlled by the user management. The user name is a unique in the user management.

Periodical password checks – 21 CFR Part 11.300 (b)

Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Within the QIAcuity Software 2.1, each password expires after 30 days and will have to be renewed after this time period. The company or laboratory operating the QIAcuity system is responsible for establishing appropriate policies and procedures in case a password renewal in less than 30 days is needed.

Loss management – 21 CFR Part 11.300 (c)

Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

N/A - This is not related to the instrument or software and need to be handled at the organizational level. User with administrator rights can reset user credentials.

Transaction safeguards – 21 CFR Part 11.300 (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.

Authorized access to the analysis and data must be secured, detected and reported by the operating system of the computer the QIAcuity Software Suite is running on. The company or laboratory operating this computer is responsible for establishing policies and procedures to prevent unauthorized use of passwords for the operating system.

Features implemented in QIAcuity Software Suite version 2.1 onwards include:

(a) After three invalid login attempts the account will be locked for 10 minutes.

(b) Any authorized access or unauthorized access attempts will be logged with username, date, time by the system in the system log audit trail.

It is in the responsibility of the user to check the audit trail for such events at an appropriate frequency.

Tests of ID devices – 21 CFR Part 11.300 (e)

Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

External devices such as tokens are not in scope of the QIAcuity software.

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.

Table 3. Responsibilities of the Company/Laboratory and QIAGEN

Regulation clause	Subject	Laboratory Company	QIAGEN	Handled by
11.10 (a)	Validation	X	X	IQ/OQ procedures are offered by QIAGEN. In addition, policies of the company or laboratory operating the QIAcuity system.
11.10 (b)	Readability		X	Existence of electronic records in human readable form that are viewable via many software programs.
11.10 (c)	Archived	X	X	All electronic records are kept within a storage space of the QIAcuity Software Suite. The Windows access control mechanism protects the modification of files within the storage space.
11.10 (d)	System security	X	X	Control of access to the QIAcuity system through user roles and individual authentication.
11.10 (e)	Audit trail	X	X	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	X	X	The QIAcuity user interface provides a guided step-by-step run setup with user confirmation.

Table 3. Responsibilities of the Company/Laboratory and QIAGEN

Regulation clause	Subject	Laboratory Company	QIAGEN	Handled by
11.10 (g)	Authority		X	Control of access to the system by individual authentication. User cannot modify electronic records
11.10 (h)	Location checks	X	X	The sample name input and experimental setup is under the responsibility and control of the company or laboratory. The system software applies checks to allow only valid information input in respective fields.
11.10 (i)	Education	X	X	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	X		Establishing and maintaining procedures to comply with this regulation is the responsibility of the company or laboratory.
11.10 (k)	System documentation	X	X	The company or laboratory operating the QIAcuity system is responsible for establishing the policies and procedures to support compliance with this regulation. The QIAcuity allows for an electronic signature when a report is created.
11.50 (a)	Signature	X	X	Printed name of a signer, date, time, and meaning are mandatory fields in the electronic signing process and need to be entered by users.
11.50 (b)	Record generation		X	Printed name of a signer, date, time, timezone offset, and meaning are part of the report and will be shown on the report pdf.
11.70	Signature/ record linking	X		Handwritten signatures is not in scope of the QIAcuity software and need to be addressed by policies of the company or laboratory operating the QIAcuity system.
11.100 (a)	Uniqueness of eSignature	X	X	The user management of the software guarantees that a combination of user name and password is unique. Policies of the company or laboratory must ensure that individuals only use their own names.
11.100 (b)	Verify identity of individuals	X	X	The user management of the software facilitates the identification of a user by name and password. Policies of the company or laboratory must ensure that passwords are kept confidential.
11.100 (c)	Legally binding signatures	X		Training of persons using electronic signatures need to be provided on an organizational level
11.200 (a)	Non biometric eSignatures		X	Providing an eSignature requires login with user name followed by a password for providing the signature.
11.200 (b)	Biometric eSignatures		N/A	The QIAcuity system does not facilitate biometric eSignatures.
11.300 (a)	Uniqueness of eSignature		X	The user management of the software guarantees that the user name required for the eSignature is unique.
11.300 (b)	Periodical password checks		X	Each password expires after 30 days and will have to be renewed after this time period.
11.300 (c)	Loss management	X		This is not related to the instrument or software and need to be handled at the organizational level.
11.300 (d)	Transaction safeguards		X	After three invalid login attempts the account will be locked for 10 minutes.
11.300 (e)	Tests of ID devices		N/A	External devices such as tokens are not in scope of the QIAcuity software