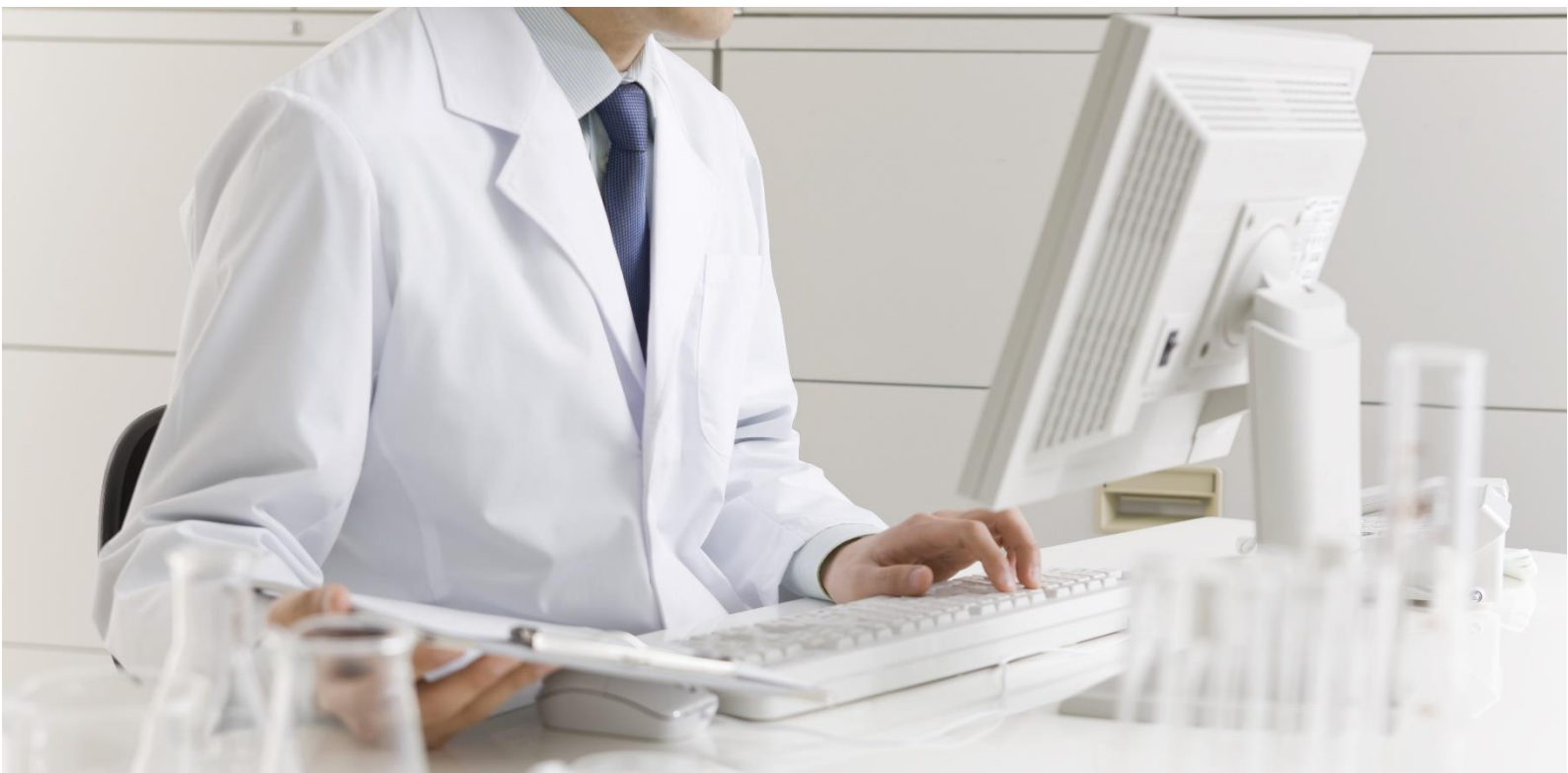


# PROQUANT 21

CFR21 part 11 module for CD60 HPTLC Densitometer



 bionis

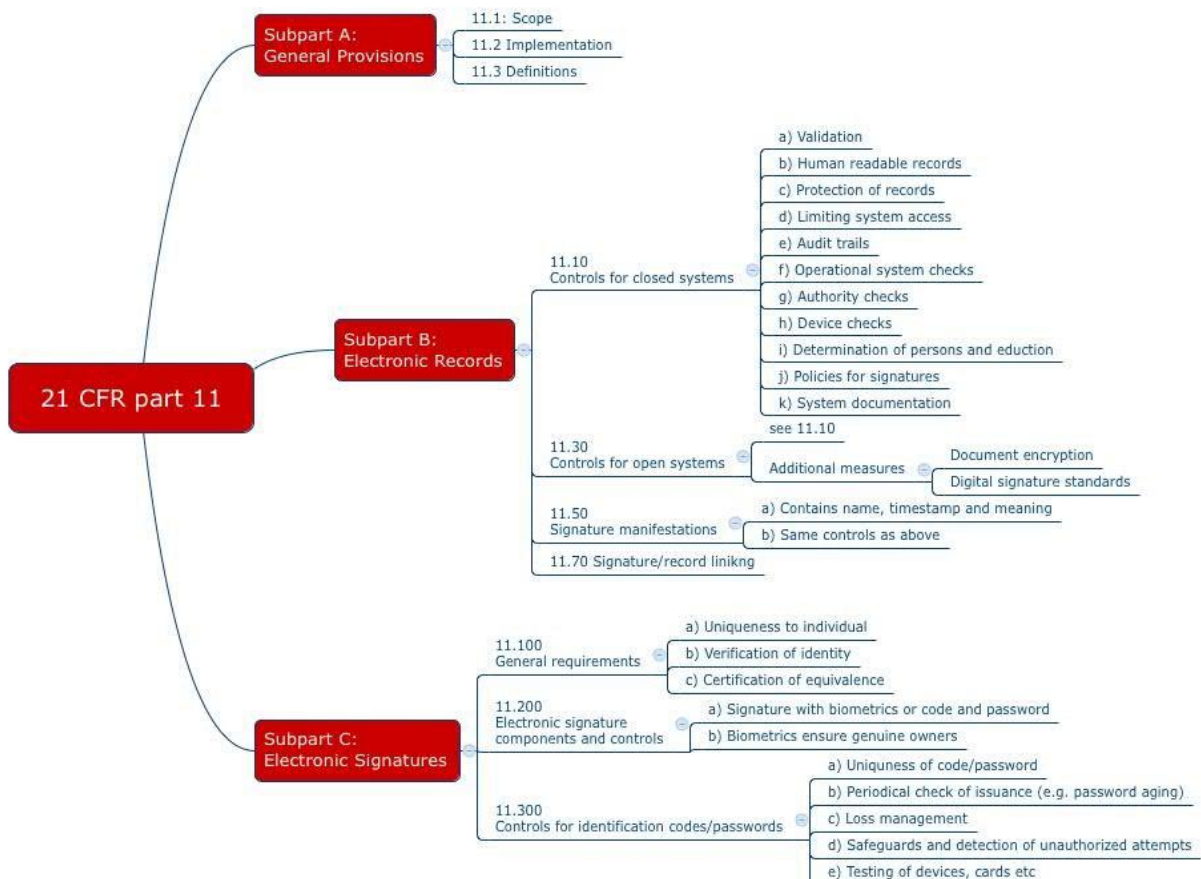
The new PROQUANT 21 module enables the use of the CD60 densitometer in accordance with CFR21 part 11 legislation.

The features to specifically meet the CFR21 part 11 regulation are divided into 2 main sections:

1. Electronic records such as data archiving and management, IT security, and IT system validation
2. Electronic signatures, i.e. the identification of signatories and ensuring the integrity of signatures

The PROQUANT 21 module meets the requirements of CFR21 part 11 point by point for densitometric analysis of samples by HPTLC.

## REQUIREMENTS TREE



## **USE OF PROQUANT 21 + PROVALID SOFTWARE**

PROQUANT 21 - Ref : BS140.096

PROVALID : Ref : BS131.816

Through the use of "ProQuant" and "ProValid" for the control, evaluation and validation of CD60 measurements, we can ensure compliance with the following requirements of 21 CFR Part 11:

1. System validation to ensure accuracy, reliability, consistency of expected performance, and the ability to discern invalid or altered records
2. The ability to generate accurate and complete copies of documents in both human-readable and electronic form
3. Document protection to enable accurate and fast retrieval throughout the life of the documents (special file formats, export and backup functions)
4. Limit access to the system to authorized individuals
5. Use of secure, computer-generated, time-stamped audit trails and methods
6. Using Methods to Apply Allowed Sequencing of Steps and Events

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a document, access the operating system or computer system's input or output device, modify a document, or perform the current operation

## A - Electronic Records

### A §11.10 Controls of Closed Systems

Persons who use closed systems to create, amend, store or transmit electronic documents must employ procedures and controls designed to ensure the authenticity, integrity and, where appropriate, confidentiality of electronic documents, and to ensure that the signatory cannot easily repudiate the signed record as not being authentic. These procedures and controls include the following:

#### **PROQUANT 21 Answer :**

According to FDA definition from subpart A §11.3 (b) (4), PROQUANT 21 is a closed system because it requires user name and password for access, which is managed by administrators.

#### **A §11.10(a)**

Systems validation to ensure accuracy, reliability, accuracy, consistency of expected performance, and the ability to discern invalid or altered records.

#### **PROQUANT 21 Answer :**

The comprehensive user administration allows access to and editing of records to be extensively set for individual users or user groups. Every change to the system and individual records is documented in detail in separate audit trails that are protected from alteration. The author of the original record also remains visible for copies.

#### **A §11.10(b)**

The ability to produce accurate and complete copies of records in a human-readable form and in an electronic electronic form, suitable for inspection, review and copying by the agency. Individuals should contact the agency if they have any questions regarding the agency's ability to review and copy electronic documents.

#### **PROQUANT 21 Answer :**

Administrators can grant access to the system. All records, including full audit trails and signatures, can be printed as a report.

#### **A §11.10(c)**

Protecting documents so that they can be retrieved easily and easily retrieved throughout the life of the documents

#### **PROQUANT 21 Answer :**

The records remain stored in a clear folder structure with filter functions until they are deliberately deleted. The permission to delete records can be restricted via the user administration.

**A §11.10(d)**

Limit access to the system to authorized individuals.

**PROQUANT 21 Answer :**

A unique user name and password are required for access. User account lockout can be manual or automated. Various policies can be set for password assignment and failed login attempts.

**A §11.10 (e)**

Use secure, computer-generated, time-stamped audit trails to independently record the date and time of inputs and operator actions that create, modify, or delete electronic records. Changes to records should not obscure previously saved information.

These audit trail documents must be retained for at least as long as that required for the electronic documents in question and must be available for review and copying by the organization.

**PROQUANT 21 Answer :**

An audit trail is generated for each record, in which all actions are recorded, including the exact time and the name of the user responsible. Audit trails are unchangeable and are only deleted together with the record. The deletion of the record and audit trail remain permanently visible as a system entry.

**A §11.10(f)**

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

**PROQUANT 21 Answer :**

Permissions can be configured to allow only specific, different users for tasks such as checking and approving records or database management.

The definition and enforcement of a specific sequence of tasks as well as the assignment of user rights is the customer's own responsibility.

**A §11.10 (g)**

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a document, access the operating system or computer system's input or output device, modify a record, or perform the current operation.

**PROQUANT 21 Answer :**

The user administration includes a detailed permission system, which can be customized for the management of all user accounts. Access can be restricted as required, and specifications for logging in and out of the system can be set at the customer's discretion.

It is the customer's own responsibility to restrict physical access to all workstations and access to the administration software.

**A §11.10 (h)**

Verification of the use of a device (e.g., terminal) to determine, if applicable, the validity of the source of data entry or operational instructions.

**PROQUANT 21 Answer :**

All access to the system is recorded and can be controlled and restricted by the system administrator, as can the permissions of individual clients.

**A §11.10 (i)**

To determine whether individuals who design, maintain or use electronic registration and electronic signature systems have the necessary education, training and experience to perform their assigned tasks.

**PROQUANT 21 Answer :**

IQ and OQ trainings are offered to qualify users in the operation of the system.

Beyond that, it is the customer's own responsibility to ensure and prove the qualification of users and administrators for their specific applications

**A §11.10 (j)**

Establishing and adhering to written policies that hold individuals accountable for actions taken under their electronic signature, in order to deter falsification of records and signatures.

**PROQUANT 21 Answer :**

The creation and enforcement of policies and procedures that support the use of the system in a regulated environment is the customer's own responsibility.

**A §11.10 (k)**

Use of appropriate controls over system documentation, including:

**A §11.10 (k) (1)**

Adequate controls over the distribution, access and use of documentation for the operation and maintenance of the system.

**PROQUANT 21 Answer :**

A comprehensive, versioned instruction manual is provided together with the system. IQ and OQ documents are additionally available.

Distribution to the users of the system, ensuring constant availability and management of the documents is the customer's own responsibility

**A §11.10 (k) (2)**

Review and change control procedures to maintain an audit trail that documents the development and modification of systems documentation on a time-based basis

**A §11.30 Controls for Open Systems**

Persons who use open systems to create, modify, maintain or transmit electronic documents must use procedures and controls designed to ensure the authenticity, integrity and, where applicable, confidentiality of electronic documents from their creation to their receipt. These procedures and controls include those identified in § 11.10, where applicable, as well as additional measures such as encryption of documents and use of appropriate digital signature standards to ensure, to the extent necessary in the circumstances, the authenticity, integrity and confidentiality of records.

**PROQUANT 21 Answer :**

This section does not apply to Proquant21, because PROQUANT 21 is a closed system by FDA definition from subpart A §11.3 (b) (4).

**A §11.50 Signature Manifestations**

**A §11.50(a)**

Signed electronic records must contain information associated with the signature that clearly indicates all of the following:

**A §11.50(a)(1)**

The signatory's printed name;

**PROQUANT 21 Answer :**

In the audit trail of a record, a description, if necessary with detailed commentary, the exact time and the name of the user responsible are recorded for all actions, in particular creation, checking and approval.

**A §11.50 (a) (2)**

The date and time the signature was signed;

**A §11.50(a)(3)**

The meaning (such as review, approval, liability, or authorship) associated with the signature.

**A §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 in any human-readable form of the electronic record (such as electronic display or print).

**PROQUANT 21 Answer :**

The audit trail can be printed with the record as well as exported as a PDF file and signed by a customer certificate.

**A §11.70 Linking Signatures and Records**

Electronic signatures and handwritten signatures executed on electronic records must be linked to their respective electronic records to ensure that the signatures cannot be deleted, copied or otherwise to falsify an electronic document by ordinary means.

**PROQUANT 21 Answer :**

Signatures are tied to the original record and are visible in the audit trail. Audit trails are protected from manipulation.

## **B - Electronic Signatures**

### **B §11.100 General requirements**

#### **B §11.100 (a)**

Each electronic signature must be unique to one person and must not be reused or reassigned to someone else.

#### **PROQUANT 21 Answer :**

The system does not allow duplicate user names. In addition, a GUID is assigned to each user. The customer can provide a certificate for each user, which they can use to export signed PDF files.

#### **B §11.100 (b)**

Before establishing, assigning, certifying, or sanctioning in any way an individual's electronic signature, or any element of that electronic signature, the organization must verify the individual's identity.

#### **PROQUANT 21 Answer :**

It is the customer's own responsibility to verify the identity of the systems users.

#### **B §11.100 (c)**

Persons who use electronic signatures must, before or at the time of such use, certify to the organization 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.

#### **PROQUANT 21 Answer :**

It is the customer's own responsibility to provide the necessary certificates.

#### **B §11.100 (c) (1)**

Certification must be submitted in paper form, signed with a traditional handwritten signature, to the Regional Operations Office (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

#### **B §11.100 (c) (2)**

Persons who use electronic signatures must, at the request of the organization, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signature signatory's handwriting.

## **B §11.200 E-Signature Components and Controls**

### **B §11.200 (a)**

Electronic signatures that are not based on biometrics must:

#### **B §11.200(a)(1)**

Use at least two separate pieces of identification, such as an identification code and password.

#### **PROQUANT 21 Answer :**

Each user account requires a user name and password to access the system. The system allows only unique user names and each account is assigned a GUID. All actions in the system are performed and thus signed by the logged-in user. In case of automatic logout due to inactivity, unlocking the system requires the password of the last logged in user.

#### **B §11.200(a)(1)(i)**

When a person executes a series of signatures within a single continuous period of controlled access to the system, the first signature must be executed using all electronic signature components; Subsequent signatures must be executed using at least one electronic signature component that is executable only by the data subject and designed to be used only by the data subject.

#### **B §11.200 (a) (1) (ii)**

When an individual executes one or more signatures that have not been completed within a single continuous period of controlled access to the system, each signature must be executed using all components of the electronic signature.

#### **B §11.200(a)(2)**

Can only be used by their true owners; and

#### **B §11.200(a)(3)**

Be administered and executed in such a way as to ensure that any attempt to use a person's electronic signature by a person other than its true owner requires the cooperation of two or more persons.

#### **PROQUANT 21 Answer :**

It is the customer's own responsibility to ensure and enforce that users keep their access data confidential and that the management of records, user accounts and system functions is independently regulated and staffed.

IT system administrators are not given direct access to the records.

**B §11.200 (b)**

Biometrics-based electronic signatures must be designed in such a way that they cannot be used by anyone other than their true owners.

**PROQUANT 21 Answer :**

Biometric signatures are not supported by the system.

**B §11.300 Controls on identification codes and passwords**

Individuals who use electronic signatures based on the use of identification codes in combination with passwords must use controls to ensure their security and integrity.

These controls include:

**11.300 (a)**

Maintain the uniqueness of each ID and password combined, so that no two people have the same ID and password combination.

**PROQUANT 21 Answer :**

The system does not allow duplicate user names.

**11,300 (b)**

Ensure that issued identification codes and passwords are periodically checked, recalled, or revised (e.g., to cover events such as the age of passwords).

**PROQUANT 21 Answer :**

User management can be customized to specify how many and which characters must be included in passwords, how long a password is valid, and how password reusability is regulated.

**11.300 (c)**

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

**PROQUANT 21 Answer :**

Tokens and similar devices that store or generate access data are not supported by the system. Through the user management, the reusability of passwords can be restricted to prevent the reuse of access data that may have become known.

**11.300 d)**

The use of transaction protection measures to prevent the unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempt to use these passwords to the system security unit and, where appropriate, for organizational management.

**PROQUANT 21 Answer :**

A maximum number of allowed failed attempts at password entry can be set in the user administration.

After reaching the individual limits, the account or workstation remains locked for a certain period of time.

Locked accounts can be unlocked only by user management administrators and workstations can be unlocked only by system administrators. Furthermore, passwords are not visible and cannot be copied in plain text when entered.

**11.300 (e)**

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

**PROQUANT 21 Answer :**

Tokens and similar devices that store or generate access data are not supported by the system.



For more informations, please contact :

**BIONIS**

6 rue de la Prévôté  
78 550 Houdan  
France

**Tel : +33 1 75 25 62 05**

**E-mail : [contact@bionis.fr](mailto:contact@bionis.fr)**

**WWW.BIONIS.FR**