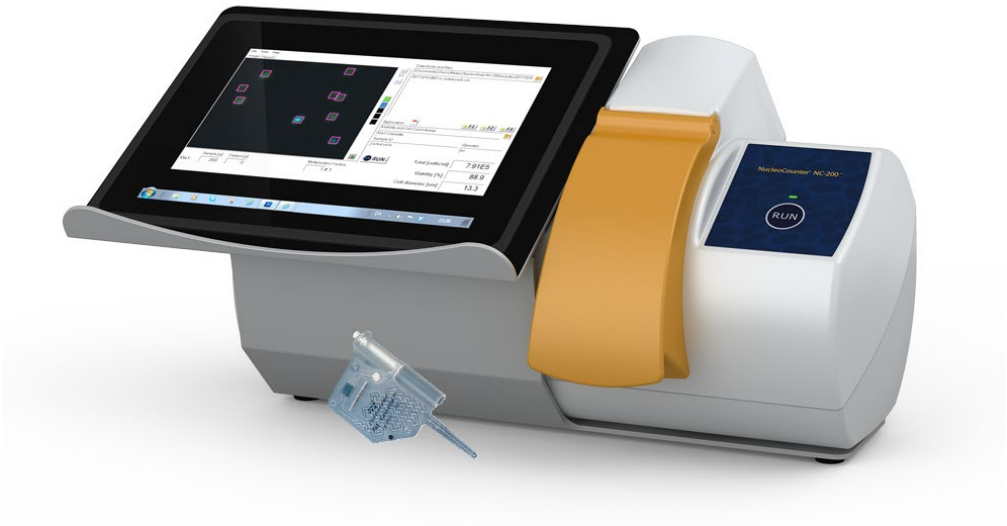
Technology that counts

chemometec

NucleoCounter® NC-200™, NucleoView™ NC-200™ Software and Code of Federal Regulation 21 Part 11; Electronic Records, Electronic Signatures (21 CFR Part 11)

A ChemoMetec A/S White Paper

August 2021



ChemoMetec A/S
Gydevang 43
DK 3450 Allerod
Denmark
Phone +45 48131020
Fax +45 48131021
contact@chemometec.com
www.chemometec.com

Table of Contents

Introduction

20th of August 1997, the US regulatory agency Food and Drug Administration (FDA) issued the 21 Code of Federal Regulation Part 11; Electronic Records, Electronic Signatures (21 CFR Part 11) as effective.

In short, the 21 CFR Part 11 defines the FDA acceptance criteria for use of electronic records and electronic signatures as equal to paper records with handwritten signatures.

NucleoCounter® NC-200™

The NucleoCounter® NC-200™ is an integrated fluorescence microscope with dual fluorescence channels designed to detect signals from cells stained with acridine orange and/or DAPI (4',6-diamidino-2-phenylindole).

The NucleoCounter® NC-200™ is a compact instrument for cell counting and viability measurement which fits perfectly in any mammalian cell laboratory performing e.g. research, quality control or monitoring of production. The NucleoCounter® NC-200™ is very simple to operate: simply load the Via1-Cassette™ and press run.

It comes with a new developed software package. The user input of optional dilution of a sample is directly accounted for in the software. The protocols can be adapted by the user to accommodate cell lines that are out of the ordinary.

How ChemoMetec A/S addresses 21 CFR Part 11

This document provides guidelines on how ChemoMetec addresses 21 CFR Part 11. The 21 CFR Part 11 regulations can only be applied when, the NucleoCounter® NC-200™ and the NucleoView™ NC-200™ software are a closed system.
Each relevant Part 11 section will be listed with number, text of the given part, resume of requirements and finally the approach taken by ChemoMetec to allow the user to meet the 21 CFR Part 11 regulation.

Section A – 21 CFR Part 11 Subpart B – Electronic Records

Part 11.10 Controls for closed systems

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:

Part 11.10 (a)

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Ensure the system can detect invalid or altered records

Data files cannot be altered from within the NucleoView™ NC-200™ software.

Additional information can however be included in the data files, which afterwards are marked.
The validity of data files are controlled via an internal checksum.

For lab-level validation, specific support can be provided by external cooperation partners.

Part 11.10 (b)

The ability to generate accurate and complete copies of records in both human readable and electronic forms suitable for inspection, review, and copying by 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.

Generate accurate records in human readable and electronic form

For inspection, review and copy by agency all results can be printed directly from the NucleoView™ NC-200™ software to the default printer only.
The default printer cannot be a file printer.

ChemoMetec A/S holds no responsibility for the further handling of exported or copied data.

All acquired data files are saved in our own .CM file format consisting of the raw image data, the calculated results and the complete settings with which the data was acquired.

Part 11.10 (c)

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

Enable accurate and easily accessible retrieval of electronic records

Data files cannot be deleted from within the NucleoView™ NC-200™ software.

Archived data files can be maintained in readily retrievable form using the combination of file servers and/or databases together with a running copy of the NucleoView™ NC-200™ software.

Part 11.10 (d)

Limiting system access to authorized individuals.

Differential access to use the NucleoCounter® NC-200™ system

Access control to the NucleoCounter® NC-200™ system relies on Windows Active Directory to assign individuals to different user groups.

Only individuals belonging to system administrators, “NucleoViewAdmin”,” NucleoViewSuperVisor” and “NucleoViewUser” user groups can access the NucleoView™ NC-200™ software.

Part 11.10 (e)

Use of secure, computer-generated time-stamped audit trails to independently record the data and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previous recorded information. Such audit trail documentation shall be retained for a period at least as that required for the subject electronic records and shall be available for agency review and copying.

Ensure audit trail for all actions made by the user, and that no records are deleted

A time-stamped Event Log automatically and continuously records all actions made by the user.

It is not possible from within the NucleoView™ NC-200™ software obscure or delete data, only adding of comments to the gathered data is possible.

The event log contains information on date, time, user name, full name, domain of computer, serial number of NucleoCounter® NC-200™ used along with type of action performed.

For each data file the user name and full name is recorded along with the serial number of the NucleoCounter® NC-200™.

Any additional information entered in a data file will be logged inside that data file with user name and time stamp, and thereby complies with the total retention period.

Archived Event Log files are encrypted and can only be opened with NucleoView™ NC-200™. The content of the Event Log are authenticated by NucleoView™ NC-200™ upon opening the Event Log file. Users assigned to the NucleoViewAdmin user groups can view the Event Log in NucleoView™ NC-200™ and export the data in CSV or PDF file format.

Part 11.10 (f)

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

Control the right sequence of steps and events

The NucleoCounter® NC-200™ system is a fully automated system, and validated to ensure that all gathering of data follows a predefined sequence defined in the protocol of the software.

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.

Control of the right of individual users to use the NucleoCounter® NC-200™ system

Access control in NucleoView™ NC-200™ software is based on Windows Active Directory and a predefined set of user groups.

The IT-manager can limit the access to authorized users.

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.

Control that the source of data input is appropriate

The NucleoCounter® NC-200™ system relies upon licenses and settings files along with predefined scripts to ensure that all steps in data acquisition are appropriate for the chosen application.

All instruments are controlled in regards to type and serial number whenever data is acquired to ensure validity of the source of data input.

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.

Proper training of all users and developers

Training in use of the NC-200™ system for data acquisition can be provided by ChemoMetec A/S. Other training in order to reach full 21 CFR Part 11 compliancy for the individual laboratories relies solely on the laboratory e.g. in cooperation with external cooperation partners.

Part 11.10 (j)

The establishment of, and adherence to, written policies that holds individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter records and signature falsification.

Provide policies to deter against falsification of records

Windows does not allow creation of two user accounts with same user name.

Local lab policies and procedures needs to ensure that there can be no reuse of user names.

The user account information is recorded within the data file for the individual creating the data file and individual(s) modifying an existing data file.

Local lab policies and procedures needs to be defined to hold individuals accountable for actions initiated under their electronic signature.

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.

System Document Control

ChemoMetec A/S follows change control and life cycle management procedures for document control.

Part 11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Controls for Open Systems

While the NucleoCounter® NC-200™ system can be operated as an open system per 21 CFR Part 11.30, Chemometec A/S encourages customers to configure the NucleoCounter® NC-200™ system a closed system.

Chemometec A/S's validation protocol only verifies that the NucleoCounter® NC-200™ system functions as a closed system and precludes the need to establish additional controls for open systems.

Part 11.50 Signature manifestations

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.

Definition of electronic signatures in data files

An individual's user name and full name along with date and time will be included as part of any electronic signature executed on data files along with the meaning of the actual signature.

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 any human readable for of the electronic record (such as electronic display or printout).

Requirements definition of electronic signatures in relation to electronic display and printouts of data

An individual's user name and full name along with date and time will be included as part of any electronic signature executed on electronic display of results and on printouts along with the meaning of the actual signature.

Part 11.70 Signature/record linking

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.

Linking of electronic signatures to their respective electronic records

The user account information is recorded within the data file for the individual creating the data file and individual(s) modifying an existing data file, herein included signing of the data file.

Section B – 21 CFR Part 11 Subpart C – Electronic Signatures

Part 11.100 General requirements

Part 11.100 (a)

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

Uniqueness of user names

Windows does not allow creation of two user accounts with the same user name.

Local lab policies and procedures shall be implemented to hinder reuse of user names.

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.

Verify identity of user

Local lab policies and procedures shall be implemented to verify the identity of individuals who will render electronic signatures.

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 legal binding equivalent of traditional handwritten signatures.
(1) The certification shall be submitted in paper form and signed with traditional handwritten signature, to 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 legal binding equivalent of the signer's handwritten signature.

Legal binding of electronic signature

Local lab policies and procedures shall be implemented to ensure that the legal formalities are followed.

Part 11.200 Electronic signature components and controls

Part 11.200 (a)

Electronic signatures that are not based upon biometrics shall:

Part 11.200 (a) (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 on 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.

Part 11.200 (a) (2)

Be used only by their genuine owners; and

Part 11.200 (a) (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

Components and design of electronic signatures

Electronic signatures are composed of user name and password for the individuals user account.

All signings will require input of user name and password along with an acceptance of the signing.

The local IT department or external cooperation partner(s) must ensure that the Windows user account is setup in a secure manner to hinder use of an individual's signature by anyone other than its genuine owner.

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.

Biometric based signatures

NucleoView™ NC-200™ software is not validated to work with electronic signatures based upon biometrics.

Part 11.300 Controls for identification codes/passwords.

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:

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.

Uniqueness of user names and passwords combinations

Windows does not allow creation of two user accounts with the same user name.

Local lab policies and procedures shall be implemented to hinder reuse of user names.

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).

Periodically verify issuance of signing credentials and properly administer users

Local lab policies and procedures shall be implemented to maintenance the signing credentials of users.

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 replacement suitable, rigorous control.

Management of potentially compromised identification codes and/or passwords

Local lab policies and procedures shall be implemented to deauthorize identification codes and/or passwords that potentially have been compromised.

Part 11.300 (d)

Use 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 system security unit, and, as appropriate to organization management.

Setup safeguards preventing and reporting unauthorized login attempts

Local lab policies and procedures shall be implemented to ensure notification of system security and as appropriate organization management in case of unauthorized attempts to use electronic signatures.

Part 11.300 (e)

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

Test of tokens and cards, which bear identification codes and passwords

Local lab policies and procedures shall be implemented to ensure that tokens and cards are checked periodically.

Glossary

CFR Code of Federal Regulation.

CM file ChemoMetec specified file containing image and data information.

CSV (comma-separated value) is a file format that stores tabular data (numbers and text) as plain text.

Full name Specified when creating a Windows user account. Usually the full name of the individual that "owns" the Windows User account.

NucleoCounter® NC-200™ system The complete system consists of a NucleoCounter® NC-200™ connected to a computer with NucleoView™ NC-200™ software installed.

NucleoView™ NC-200™ Software NucleoView™ NC-200™ software is used to control the NucleoCounter® NC-200™ and to interpret and analyze the data acquired by use of the System .

NucleoView™ user levels Access to certain features within the NucleoView™ NC-200™ software are controlled by Windows Active Directory by assignment of users to one of three possible user levels; NucleoViewAdmin, NucleoViewSuperVisor and NucleoViewUser.

Login name and User name Two words with same meaning used interchangeably. Primary name used to define a Windows user account; must be entered together with user password when logging onto the computer. Also the name used in combination with the user password for electronic signatures.

User account A record that consists of all information that defines a Windows user, including the user name, password and full name of the individual along with information on the user group the individual belongs to.

User password Secret code that in combination with the user name allows individuals with a user account to log onto the computer.

Windows Active Directory Centralized domain management system.

Product Notes

The NucleoCounter® NC-200™ system is intended FOR RESEARCH USE ONLY. NOT FOR DIAGNOSTIC OR THERAPEUTIC USE.
To reach full compliancy it relies upon the customer to implement Standard Operational Procedure (SOP), Technical Procedure (TP), training of individuals etc.

Disclaimer Notices

The material in this document and referred documents is for information only and is subject to change without notice. While reasonable efforts have been made in preparation of these documents to assure their accuracy, ChemoMetec A/S assumes no liability resulting from errors or omissions in these documents or from the use of the information contains herein.

ChemoMetec A/S reserves the right to make changes in the product without reservation and without notification to its user.

ChemoMetec A/S assumes no liability regarding the cited text from the 21 CFR Part 11 regulative and always directs the reader to FDA for correct and full information regarding all of the 21 CFR Part 11 regulations.

All responsibilities for work done by external cooperation partners rely solely on these partners.

Trademarks

ChemoMetec and NucleoCounter® are registered trademarks owned by ChemoMetec A/S.
NucleoCounter® NC-200™, NucleoView™ and Via1-Cassette™ are trademarks of ChemoMetec A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation in United States and other countries.