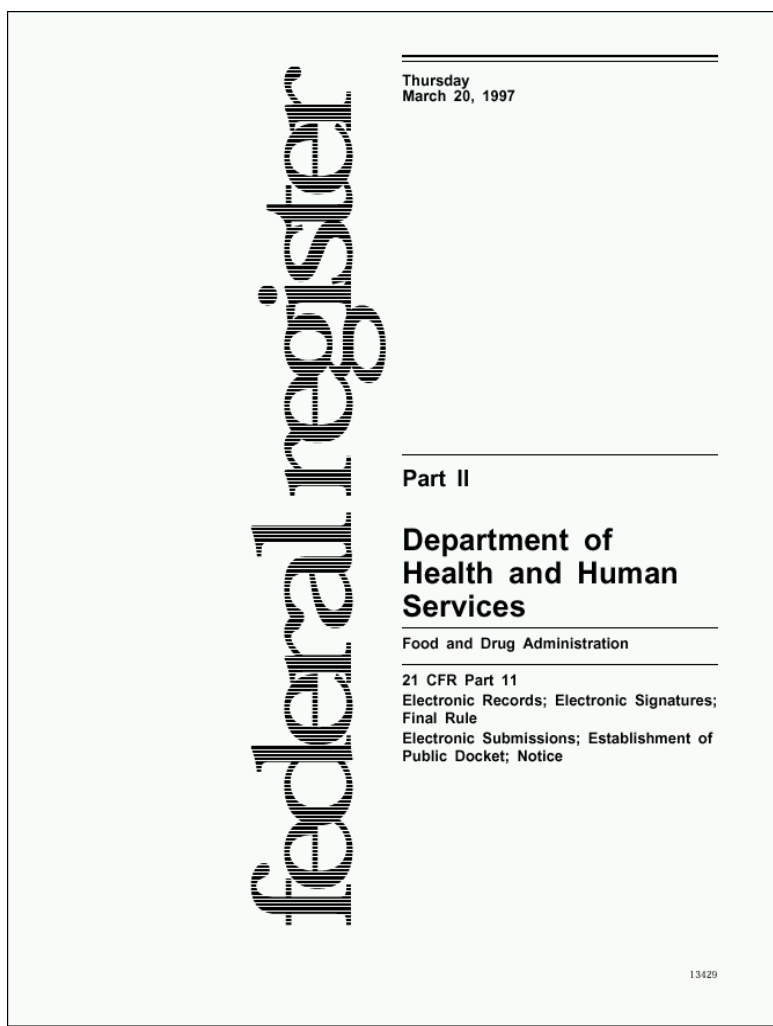


PerkinElmer Turbochrom Client/Server and Workstation Software



Support for Electronic Records and Electronic Signature



What is 21 CFR Part 11?

Title 21 of the Code of Federal Regulations (CFR) is the Section of the United States government Rules and Regulations document that deals with the Food and Drug Administration (FDA). Chapter I, Part 11 of this Section applies to records in electronic form and to the criteria under which the FDA will consider electronic records and signatures

"to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper".

This final ruling, published on March 20, 1997 and in effect since August 20, 1997, is another step in the process of determining how to accommodate "paperless" record systems under the current *Good Manufacturing Practice* regulations in 21 CFR Parts 210 and 211.

The ultimate goal is to provide the formal regulations for the submission of required documents to the agency [the FDA] in electronic format.

What is the purpose of this PerkinElmer document?

The purpose of this document is to describe the relevant portions of the 21 CFR Part 11 regulations and to explain their implementation using the Turbochrom Client/Server and Workstation software.

It is critical to understand that such support is not entirely the responsibility of PerkinElmer and the Turbochrom software. As defined in the specifications of 21 CFR Part 11, it is also the responsibility of the persons using and implementing electronic records and electronic signatures to *"employ procedures and controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records"*. Proper procedures and practices are as much a part of overall compliance with these regulations as are the features of the Turbochrom software.

What are electronic records?

In Subpart A of the regulations, Section 11.3 deals with definition of the terms used in the rest of the document. Under these definitions, *"electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system"*.

In practical terms, this refers to any computer information submitted to the agency, or any information not submitted but required to be maintained. Public Docket No. 92S-0251, in the same issue of the Federal Register (Vol. 62, No. 54), identifies the types of documents acceptable for submission in electronic

form and where such submissions may be made.

Are electronic records and electronic signatures required by the FDA?

As described in preamble to this final ruling, *"The use of electronic records as well as their submission to FDA is voluntary."* In the General Comments section of the ruling, it is further stated that *"The agency emphasizes that these regulations do not require, but rather permit, the use of electronic records and signatures."*

The agency is currently preparing to accept electronic submissions from all its program areas. Subpart A, Section 11.2 indicates that *"persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures ... provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251"*.

The intention of this provision is to allow firms not prepared for electronic record keeping to continue the use of *"traditional signatures and paper documents"*. Organizations that do choose to implement electronic records and electronic signatures, however, must comply fully with all aspects of these regulations. Likewise, all records to which this ruling applies are subject to these regulations. Support for electronic records cannot be applied selectively.

Does Turbochrom provide all the necessary electronic records?

As a vendor, PerkinElmer is not required to provide all of the electronic information a regulated organization needs to maintain or submit to the agency. It would be extremely difficult for any one vendor to do so.

For example, a part of the electronic submission for drug approval is the labeling text, which includes all text, tables, and figures proposed for use in the package insert. PerkinElmer does not provide software to produce this kind of information. Similarly, Turbochrom does not provide the kind of information

required for the documentation of clinical trial results.

An organization that chooses to implement electronic records, however, is required to provide the agency with all such documents in a form consistent with these regulations. The parts of the overall electronic documentation for which Turbochrom is responsible must comply with all the regulations relevant to those records, as described in 21 CFR Part 11.

How are electronic records and electronic signatures implemented?

Under the definitions in Subpart A, Section 11.3, two classes of system are described: *"closed systems"* and *"open systems"*. A closed system is one *"in which system access is controlled by persons who are responsible for the content of electronic records"*. In other words, the people and organization responsible for creating and maintaining the information on the system are also responsible for operating and administering the system. In contrast, an open system is one *"in which system access is not controlled by persons who are responsible for the content of electronic records"*.

In a typical Turbochrom implementation, the use, operation, maintenance and administration of the system is controlled by strict procedures developed for system security and data integrity by the end-user's organization. Anyone who interacts with the system, from system administrators to Turbochrom users, must abide by those procedures. Even though these functions may be split between several different departments within the same organization, the overall responsibility for the system resides within that organization. This is an example of a *"closed"* system.

Where control and operational maintenance of the system are *"outsourced"* to another organization, such as with a time-sharing service or a commercial *"server farm"*, the system is considered to be *"open"*. The controls governing the operation of a system in these two situations are overlapping, but for an open system, additional safeguards are required.

What are the controls for electronic records?

Subpart B, Section 11.10 describes the controls to be applied to a *"closed system"*. Section 11.30 describes the controls for an *"open system"*, which include *"those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards"*. Since a typical Turbochrom system can be regarded as a closed system, additional controls for open systems will not be discussed in this document.

The primary thrust of these controls is *"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"*. In other words, to protect the data and to make it difficult for someone to say that this is not their *"signature"*.

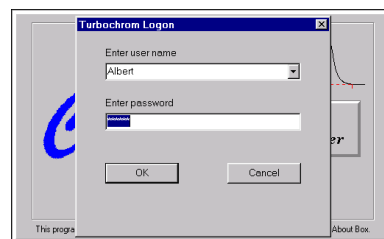


Figure 1. The Turbochrom Login

Many of the controls described in Section 11.10 refer to written procedures (SOP's) required of an organization by the agency, for the purpose of data storage and retrieval, access control, training, accountability, documentation, record keeping, and change control. The other controls are addressed either by the Turbochrom software itself, or in combination with end-user procedures.

Of the other controls, perhaps the foremost is described in Section 11.10 Paragraph (a): *"Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."* It is the complete and overall validation of the system, as developed by the organization, which ensures the integrity of the system and the data within. It is to this end that the features of the Turbochrom software comply with the specifications of these regulations.

How does Turbochrom provide these controls?

The Turbochrom software employs a system of usernames and passwords, consistent with the specifications of Subpart C, Section 11.300, "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" (Figure 1). Additionally, the level of access to the Turbochrom system is controlled by the rights granted through the "permissions" of the Turbochrom "Job Type" to which a user is assigned.

Turbochrom also performs data input and "operational checks", as specified in Subpart B, Section 11.10, "to determine, as appropriate, the validity of the source of data input or operational instruction", and "to enforce permitted sequencing of steps and events". These two features ensure that, as much as possible, valid data are being entered into the system, and all required steps have been completed to perform the task at hand.

The purpose of all such data checking and validation is described in Section 11.10, Paragraph (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". Consequently, strict procedures can be enforced within a Turbochrom system to record all changes that are made to data generated from within Turbochrom, as defined in Section 11.10, Paragraph (e).

Any file created by Turbochrom can have audit trailing enabled. Likewise, Turbochrom can be configured to automatically force audit trailing for all new files. Once auditing has been enabled for a file, it cannot be disabled, nor can it be bypassed. Under these conditions, all changes made to a file are automatically recorded. These changes consist of "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".

When a change to a file is detected, Turbochrom automatically records the identity of the user making the change, the date and timestamp of the change, the

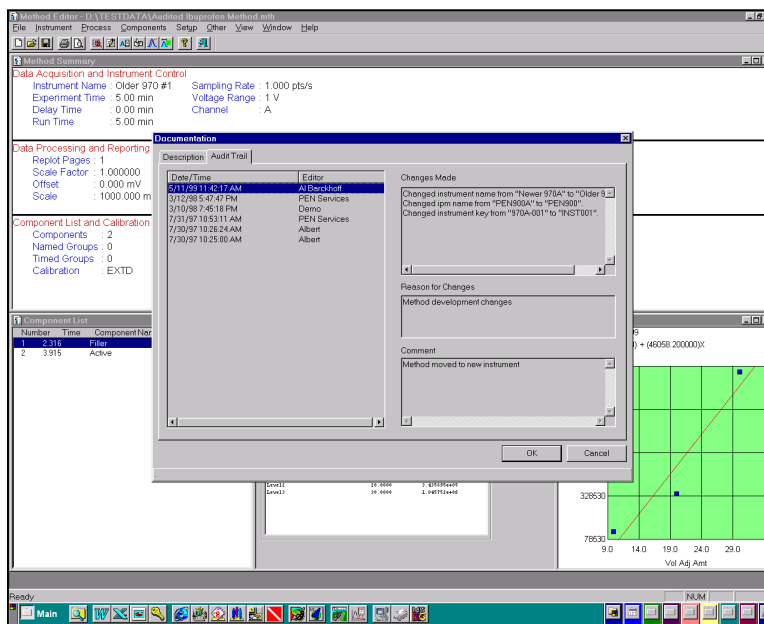


Figure 2. Reviewing the method Audit Trail

parameter that has changed, the old value and the new value. The user also may be required to enter a "reason" for the change, selected from a pre-defined list, as well as any free text comments regarding the change (Figure 2).

The complete audit trail is then stored inside the modified file itself, such that "record changes shall not obscure previously recorded information", and in a "form suitable for inspection, review, and copying by the agency". In other words, a complete and continuous record of all changes is maintained. Through the file protection and archiving capabilities of a Turbochrom system, it can be ensured, in compliance with Section 11.10, Paragraph (e), that "Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records".

What is an electronic signature?

In Subpart A, Section 11.3, an electronic signature is defined as "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature". Subpart C, Section 11.100 of the regulation defines the general requirements of such a manifestation. Paragraph (a) states that "each electronic

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

These two paragraphs, taken together, mean that an electronic signature is some computer representation of a user's identity, developed to insure the distinct and unique identity of that user.

The procedural aspect of Section 11.100 requires that before any such electronic representation is applied, the organization first must "verify" the identity of that individual. The subsequent use of electronic signatures as the "legally binding equivalent of traditional handwritten signatures" then must be "certified" to the agency in writing.

How can electronic signatures be produced?

Subpart C, Section 11.200, refers to biometric and non-biometric forms of electronic signature. Biometric signatures are defined in Subpart A, Section 11.3 as a "a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable". Biometrics are generally regarded as techniques such as fingerprints or retinal scans, which are considered to be totally unique to each

individual and require specific forms of scanning devices to read and interpret.

Non-biometric signatures are those that are computer generated and, as per Section 11.200, "Employ at least two distinct identification components such as an identification code and password". It is this form of electronic signature that is supported by the Turbochrom software.

How does Turbochrom support electronic signatures?

The Turbochrom software employs User ID's and passwords to verify the identification of each user logging into the Turbochrom system. When using this technique, Subpart C, Section 11.300 of the regulation requires "maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password". This section also requires that the "identification code and password issuances are periodically checked, recalled, or revised". Turbochrom software supports both of these provisions.

The administration of a Turbochrom system requires that individuals be added to the database of valid Turbochrom users. The "identification code" or username of each Turbochrom user must be unique. No two users on the same Turbochrom system can have the same username. It is also required that these users supply a password to access the Turbochrom software, thus satisfying the requirement to "employ at least two distinct identification components such as an identification code and password".

Passwords can be controlled to prohibit the use of duplicates and to force the selection of new passwords after a prescribed period of time. By the implementation of these features, Turbochrom can satisfy the requirement that "identification code and password issuances are periodically checked, recalled, or revised".

When a Turbochrom system is configured to link its security to that of the Windows NT[®] operating system, the additional specification of "transaction safeguards to prevent unauthorized use of passwords and/or identification codes" can be satisfied. Attempts at

"unauthorized use" can be detected and further prevented by automatically "locking-out" a user account after a set number of failed attempts to log into that account, and by recording such activities in the system transaction logs.

How are electronic signatures applied?

Subpart C, Section 11.200 stipulates several requirements for the control of electronic signatures. Procedurally, the regulations require that electronic signatures "be used only by their genuine

performed during a single, continuous period of controlled system access". This section of the document represents the "heart" of electronic signature application.

To comply with these provisions, Turbochrom uses the application of the username and password to authenticate the user making and saving the changes, in conjunction with audit trailing, "to independently record the date and time of operator entries and actions that create, modify, or delete electronic records" (Figure 3).

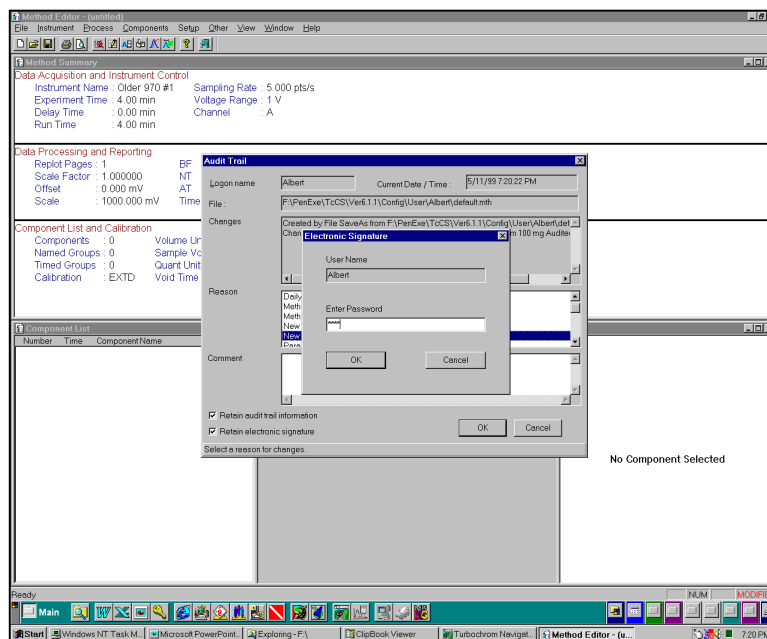


Figure 3. Enabling Audit Trail and Electronic Signature in a new method

owners" and that they "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". Through the application of Turbochrom user and password configuration procedures, the system can be configured to "ensure" that inappropriate use of these identifiers can be performed only by the intentional divulgence of security information.

Section 11.200 further specifies the use of electronic signature components during a period "when an individual executes a series of signings during a single, continuous period of controlled system access", and "when an individual executes one or more signings not

How does Turbochrom put all this together?

Subpart B, Sections 11.50 and 11.70 are the segments of 21 CFR Part 11 that substantiate the electronic signatures and link them "to their respective electronic records". It is with these controls that a "signed" electronic record becomes complete. It is through the combination of all the Turbochrom controls described within this document, as well as the ability to display, preview, print, archive and retrieve Turbochrom data on demand, that provides this functionality and complies with these specifications.

The final rule is available electronically via Internet: <http://www.fda.gov>.