

DATATRACE[®] Compliance with 21 CFR Part 11

Subpart B Electronic Records

§ 11.10 Controls for closed systems.

	21 CFR Part 11 Guideline	DATATRACE[®] for Windows Compliance
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	All versions of the DATATRACE [®] for Windows (DTW) program are subjected to a rigorous validation program before release. The DTW program, through various security checks and encryption algorithms, protects and tests for any corruption to collected data. Specifically, the user at no time has direct access to the originally collected data, and therefore, has no access to modify the original data profile.
(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.	The DTW program creates data records that can not be modified and stored in a format that can only be accessed through the DTW software. Following internal security verification, copies of the collected data can be reproduced for regulatory inspection and review.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The DTW program through various security checks and encryption algorithms protects and tests for any corruption to collected data. This function continues as long as the data is resident in the DTW system.
(d)	Limiting system access to authorized individuals.	DTW password protection includes sophisticated encryption algorithms to secure and safeguard access to the system by only those that have been authorized to do so. Various levels of access are available to limit accessibility to specified system components.
(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.	DTW provides a date/time stamped audit trail of all data creation and deletion functions. DTW also logs any movement of data to external locations and/or all Archive and Restore functions. The audit trail is a non-modifiable record that lists audited functions from the original installation date of the DTW software. The audit trail record is accessible for regulatory review and copying.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	NOT APPLICABLE

Subpart B Electronic Records (cont.)

§ 11.10 Controls for closed systems (cont.).

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
(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.	DTW password protection includes sophisticated encryption algorithms to secure and safeguard access to the system by only those that have been authorized to do so. Various levels of access are available to limit accessibility to specified system components. No original data record can be modified or altered in the DTW system, nor can manual or hand-generated data or records be inserted into the DTW system.
(h)	Use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Source data can only be generated within the DTW program, which is password protected and includes data encryption.
(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.	NOT APPLICABLE
(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.	NOT APPLICABLE
(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.	NOT APPLICABLE

Subpart B Electronic Records

§ 11.30 Controls for open systems.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
(a)	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 standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	NOT APPLICABLE

Subpart B Electronic Records (cont.)

§ 11.50 Signature manifestation.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
(a)	<p>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p> <ol style="list-style-type: none"> (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. 	<p>DTW requires the use of the appropriate User ID/Password when using the program. Based on the designated level of authorization, the users electronic signature will be displayed with all of the required items:</p> <ol style="list-style-type: none"> (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.
(b)	<p>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),</p>	<p>DTW requires the use of the appropriate User ID/Password when using the program. Based on the designated level of authorization, the users electronic signature will be displayed with all of the required items:</p> <ol style="list-style-type: none"> (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.

§ 11.70 Signature/record linking.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
	<p>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.</p>	<p>DTW requires the use of the appropriate User ID/Password when using the program. These codes are encrypted and stored in the DTW program and are not accessible or modifiable by users, including the system administrator. All reports generated by DTW are include electronic signatures that are verified before the electronic signatures are included on the report.</p>

Subpart C Electronic Signatures

§ 11.100 General requirements.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	DTW password assignments are unique to an individual as assigned by the designated system administrator. The password must be at least eight (8) characters with at least one of them numeric. No previously used User ID and password combination can be reassigned.
(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.	NOT APPLICABLE
(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.	NOT APPLICABLE

Subpart C Electronic Signatures (cont.)

§ 11.200 Electronic signature components and controls.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
(a)	<p>Electronic signatures that are not based upon biometrics shall:</p> <p>(1) Employ at least two distinct identification components such as an identification code and password.</p> <p>1) 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.</p> <p>2) 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.</p>	<p>DTW password assignments are unique to an individual as assigned by the designated system administrator. After the initial sign in the owner must change their password to at least eight (8) characters with at least one of them numeric.</p> <p>During a single, continuous period of controlled system access, DTW requires the use of both the user ID and password. Subsequent signings require only one of the components.</p> <p>Both components are required where either 15 minutes has elapsed since the last activity or during multiple sessions when a new session has been initiated.</p>
	(2) Be used only by their genuine owners; and	NOT APPLICABLE
	(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.	DTW allows no one, including the System Administrator, to know users passwords. After a user performs their initial sign in, the user is required to change their password. The new password is not known by any one other than the genuine owner.
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	NOT APPLICABLE

Subpart C Electronic Signatures (cont.)

§ 11.300 Controls for identification codes/passwords.

	21 CFR Part 11 Guideline	DATATRACE® for Windows Compliance
	<p>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 control shall include:</p> <p>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.</p>	<p>DTW requires the system administrator to enter a unique user ID. The DTW password assignments are unique to an individual where each password must have a minimum of eight (8) characters with at least one of them numeric.</p> <p>Duplicate user ID and password combinations are not allowed by DTW in any form.</p>
	<p>b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p>NOT APPLICABLE</p>
	<p>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.</p>	<p>NOT APPLICABLE</p>
	<p>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.</p>	<p>The DTW audit trail logs all log in attempts, successful or not. The audit trail report is available to authorized individuals for review and verification.</p>
	<p>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.</p>	<p>NOT APPLICABLE</p>

Relevant Definitions:

A **Closed System** is defined as "... an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."

An Open **System** is defined as "... an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."

Biometrics is defined as "... 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 the individual and measurable."