

# Cardiff Intelligent Documents in the Pharmaceutical Industry: 21 CFR Part 11 Compliance

Cardiff White Paper



# Cardiff Intelligent Documents in the Pharmaceutical Industry: 21 CFR Part 11 Compliance

July 2006

## Table of Contents

<b>Cardiff Intelligent Documents in the Pharmaceutical Industry: 21 CFR Part 11 Compliance</b> . . . .	<b>3</b>
<b>Subpart A – Electronic Records</b> . . . . .	<b>3</b>
11.10 Controls for Closed Systems . . . . .	3
11.30 Controls for open systems . . . . .	5
11.50 Signature Manifestations . . . . .	5
11.70 Signature/ Record Linking . . . . .	5
<b>Subpart B – Electronic Signatures</b> . . . . .	<b>5</b>
11.100 General Requirements . . . . .	5
11.200 Electronic signature components and controls . . . . .	6
11.300 Controls for identification codes/ passwords . . . . .	6

Publisher's Note: Information contained in this document is intended for guideline purposes only. Cardiff product documentation supersedes information contained in this document. The situations described in this document are offered as examples; actual configurations and results will vary from system to system.

---

# Cardiff Intelligent Documents in the Pharmaceutical Industry: 21 CFR Part 11 Compliance

Title 21 of the Code of Federal Regulations Part 11 (21CFR11) defines the rules for electronic records and electronic signatures for pharmaceutical companies<sup>1</sup>.

Cardiff has developed a solution, ClinCapture, that allows pharmaceutical and biotechnology companies to conduct hybrid paper-electronic clinical trials. ClinCapture integrates two applications: TeleForm, a paper content capture system, with LiquidOffice, a business

process management system. The ClinCapture solution allows users to capture data from either paper and/or electronic clinical forms, streamline the clinical trials process and increase clinical efficiencies.

This white paper is a clause-by-clause analysis of the requirements of 21 CFR Part 11 and how these requirements relate to Cardiff TeleForm.

Section	Requirement	TeleForm Implementation
---------	-------------	-------------------------

## Subpart A – Electronic Records

11.10	Controls for Closed Systems	
	System owners 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, as defined in sections 11.10.	<b>The design, development, manufacturing and lifecycle management of TeleForm is done according to guidelines specified in the Cardiff Software Development Processes and Guidelines document. These products provide and guarantee authenticity, integrity and confidentiality of electronic records and electronic signatures, and are ready to be integrated in a 21 CFR Part 11 compliant system.</b>
(a)	The system owner shall validate the system to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	<b>Note that although TeleForm complies with 21 CFR Part 11 requirements where applicable, ultimate responsibility for 21 CFR Part 11 rests with persons responsible for electronic record content, just as the responsibility for compliance with paper record requirements generally lies with those responsible for the record's content.</b>
(b)	The system shall generate accurate and complete copies of records in human readable and electronic form suitable for inspection, review and copying.	<b>The system maintains complete and accurate electronic copies of all records, including the initial scanned record, which can be viewed and/or printed on demand.</b>
(c)	The system owner shall establish and adhere to written procedures to ensure protection of records to enable their accurate and ready retrieval throughout the records retention period.	<b>The validation of their applications and processes is the responsibility of the software purchaser.</b>
(d)	The system shall limit system access to authorized individuals.	<b>While TeleForm fully employs predefined role-based security via LDAP, it is the responsibility of the software purchaser to enable the security setting in TeleForm and connect TeleForm to an LDAP system.</b>  <b>Note: When security is controlled by the Software Purchaser's LDAP system, no two users maybe created with the same username/password combination, nor can they be deleted once they log in. Appropriate security for open systems, password configuration and expiration settings, safeguards against unauthorized use of username/password and detection and reporting of privileges and unauthorized use of username/password functionalities are employed.</b>

<sup>1</sup> No software vendor can be certified as Part 11 compliant. However, a software vendor can offer technical control features for 21 CFR Part 11 compliance. Please note that it is the responsibility of the organization to implement FDA Regulation 21 CFR Part 11 correctly and consistently.

Section	Requirement	TeleForm Implementation
(e)	The system shall employ secure, computer-generated date/time-stamped audit trails to independently record operator entries and actions that create, modify, or delete electronic records, without obscuring previously recorded information.	<p><b>TeleForm enables full audit tracking functionality so that every image and data view and manipulation is recorded and retrievable for later reporting. It is the responsibility of the software purchaser to connect TeleForm to an RMS as all audit trail records are exported from the TeleForm system along with the images and their data.</b></p> <p><b>Note: When clinical trial applications utilizing TeleForm connect to a RMS, TeleForm is used as the data entry front-end of the solution. The RMS is responsible for records archiving, versioning and display. All data and incremental changes to information, including form images, clinical trial related data, audit and signature information, are exported to the RMS, with a pointer to the image, wherever that image may be stored (outside of TeleForm). The RMS record is considered the single source from which this information is viewed and managed.</b></p>
(f)	The system shall enforce required steps and events sequencing, as appropriate (e.g., key steps cannot be bypassed or similarly compromised).	<b>System fully supports event sequencing functionality, through the creation of workflows.</b>
(g)	The system shall 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.	<p><b>While TeleForm fully employs predefined role based security via LDAP, it is the responsibility of the software purchaser to enable the security setting in TeleForm and connect TeleForm to an LDAP system.</b></p> <p><b>Note: When security is controlled by the Software Purchaser's LDAP system, no two users maybe created with the same username/password combination, nor can they be deleted once they log in. Appropriate security for open systems, password configuration and expiration settings, safeguards against unauthorized use of username/password and detection and reporting of privileges and unauthorized use of username/password functionalities are employed.</b></p>
(h)	The system shall determine, as appropriate, the validity of the source of data input or operational instruction.	<b>System only receives data through TeleForm installed workstations. Once the data is processed and transferred to the software purchaser's document management system, a validity check should be performed by the document management system.</b>
(i)	The system owner shall determine that people, who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	<b>This is the responsibility of the software purchaser.</b>
(j)	The system owner shall establish and adhere to written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	<b>This is the responsibility of the software purchaser.</b>
(k)	<p>Use of appropriate controls over systems documentation including:</p> <p>(1) The system owner shall establish and adhere to adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</p> <p>(2) The system owner shall establish and adhere to revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<b>This is the responsibility of the software purchaser.</b>

Section	Requirement	TeleForm Implementation
<b>11.30</b>	<b>Controls for open systems</b>	
	System owners 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 such additional measures as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality, as defined in section 11.50.	<p><b>While TeleForm fully employs predefined role based security via LDAP, it is the responsibility of the software purchaser to enable the security setting in TeleForm and connect TeleForm to an LDAP system.</b></p> <p><b>Note: When security is controlled by the Software Purchaser's LDAP system, no two users may be created with the same username/password combination, nor can they be deleted once they log in. Appropriate security for open systems, password configuration and expiration settings, safeguards against unauthorized use of username/password and detection and reporting of privileges and unauthorized use of username/password functionalities are employed.</b></p> <p><b>For Web-based workstations additional LDAP security control should be enabled.</b></p>
<b>11.50</b>	<b>Signature Manifestations</b>	
(a)	<p><b>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</b></p> <p>(1) The printed name of the signer; and</p> <p>(2) The date and time when the signature was executed; and</p> <p>(3) The meaning (such as review, approval, responsibility, or authorship associated with the signature).</p>	<p><b>It is the responsibility of the software purchaser to connect TeleForm to an RMS system since TeleForm is used as the data entry front-end of the solution. The RMS is responsible for records archiving, versioning and display. All data and incremental changes to information, including form images, clinical trial related data, audit and signature information, are exported to the RMS, with a pointer to the image, wherever that image may be stored (outside of TeleForm), and the RMS record is considered the single source from which this information is viewed and managed.</b></p>
(b)	The system shall ensure the three signature elements (described in the previous requirement) of a signed electronic record are a part of any human readable form of the electronic record (e.g., electronic display or printout).	<p><b>The user ID and password used in the system are "e-Signatures" and no non e-Signature user ID and passwords are used. Additionally, a user is prompted for e-Signature prior and subsequent to all data entry. Signature information is captured and maintained throughout the workflow and document retention. All signed records include printed name of the signer, date/time signature was executed, and the meaning associated with the signature (e.g., approval, responsibility, authorship).</b></p>
<b>11.70</b>	<b>Signature/ Record Linking</b>	
	The system shall ensure electronic signatures are linked to their respective electronic records and that these electronic signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	<p><b>System has a common index tracking number functionality that will be used to associate the exported image with its corresponding exported form data, e-Signature, and audit information.</b></p>

### Subpart C – Electronic Signatures

Section	Requirement	TeleForm Implementation
<b>11.100</b>	<b>General Requirements</b>	
(a)	The system shall ensure that each electronic signature is unique to one individual and shall not be reused by, or reassigned to, anyone else.	<p><b>It is the responsibility of the software purchaser to connect TeleForm to an RMS since TeleForm is used as the data entry front-end of the solution. The RMS is responsible for records archiving, versioning and display. All data and incremental changes to information, including form images, clinical trial related data, audit and signature information, are exported to the RMS, with a pointer to the image, wherever that image may be stored (outside of TeleForm), and the RMS record is considered the single source from which this information is viewed and managed.</b></p>
(b)	The system owner shall verify the identity of an individual prior to the establishing, assigning, certifying or otherwise sanctioning an individual's electronic signature, or any element of such electronic signature.	<p><b>This is the responsibility of the software purchaser.</b></p>

Section	Requirement	LiquidOffice Implementation
(c)	<p>The system owner shall certify to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures, prior to using electronic signatures.</p> <p>(1) The system owner shall submit this certification in hand signed paper format to Office of Regional Operations (HFC- 100), 5600 Fishers Lane, Rockville, MD 20857.</p> <p>(2) The system owner 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.</p>	<p><b>This is the responsibility of the software purchaser.</b></p>
<b>11.200</b>	<b>Electronic signature components and controls</b>	
(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>(i) The system shall require the use of all electronic signature components for the first signing during a single continuous period of controlled system access; the system shall allow all subsequent signing during the same continuous period of controlled system access to use at least one electronic signature components; the system shall ensure users are timed out during periods of specified inactivity.</p> <p>(ii) The system shall require the use of all electronic signature components for the signings not executed during a single continuous period of controlled system access.</p> <p>(2) ensure non-biometric electronic signatures can only be used by their genuine owner.</p> <p>(3) require all attempts use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><b>The user ID and password used in the system are “e-Signatures” and no non e-Signature user ID and passwords are used. Additionally, the user is prompted for e-Signature prior and subsequent to all data entry. Signature information is captured and maintained throughout the workflow and document retention. All signed records include printed name of the signer, date/time signature was executed, and the meaning associated with the signature (e.g., approval, responsibility, authorship).</b></p> <p><b>No user has access to read another user’s password. Forced password change on first login after administrator has set or reset the password.</b></p>
(b)	<p>The system shall ensure biometrics electronic signatures can only be used by their genuine owner.</p>	<p><b>TeleForm does not support biometric signatures.</b></p>
<b>11.300</b>	<b>Controls for identification codes/ passwords</b>	
	<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 controls shall include:</p>	<p><b>It is the responsibility of the software purchaser to connect TeleForm to an LDAP system.</b></p> <p><b>Note: When security is controlled by the Software Purchaser’s LDAP system, no two users maybe created with the same username/password combination, nor can they be deleted once they log in. Appropriate security for open systems, password configuration and expiration settings, safeguards against unauthorized use of username/password and detection and reporting of privileges and unauthorized use of username/password functionalities are employed.</b></p>

(a)	The system shall require each combination of identification code and passwords are unique, such that no two individuals have the same combination of identification code and password.	<b>It is the responsibility of the software purchaser to connect TeleForm to an LDAP system.</b>
(b)	The system shall required passwords to be periodically revised. The system owner shall establish and adhere to procedures, which control the issuance and recall of identification codes.	<b>It is the responsibility of the software purchaser to connect TeleForm to an LDAP system.</b>
(c)	The system owner shall establish and adhere to loss management procedures which document the electronic deauthorization of lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information as well as the measures to issue temporary or permanent replacements using suitable, rigorous controls.	<b>This is the responsibility of the software purchaser. Cards or tokens are not used.</b>
(d)	The system shall employ transaction safeguards preventing the unauthorized use of password and/or identification codes.  The system shall detect and report unauthorized use of password and/or identification codes to specified units.	<b>It is the responsibility of the software purchaser to connect TeleForm to an LDAP system.</b>
(e)	<b>The system owner shall establish and adhere to a procedure which allows for the 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.</b>	<b>Cards or tokens are not used.</b>

Related Documentation. For more information about using Cardiff TeleForm and LiquidOffice in the pharmaceutical industry, visit our website at [www.cardiff.com/solutions/industry\\_solutions/life\\_sciences/](http://www.cardiff.com/solutions/industry_solutions/life_sciences/).

---

**Cardiff (USA)**

3220 Executive Ridge  
Vista, CA 92081  
**Tel:** 760.936.4500  
**Fax:** 760.936.480

**Email:** [information@cardiff.com](mailto:information@cardiff.com)

**Cardiff (UK)**

Cambridge Business Park,  
Cowley Rd, Cambridge CB4 0WZ, UK  
**Tel:** +44 (0) 1223 448 000  
**Fax:** +44 (0) 1223 448 001

**Email:** [information@cardiff.com](mailto:information@cardiff.com)

**Other Offices**

Cardiff has additional offices in Boston, New York, Sunnyvale, Vista and Washington DC, as well as in Amsterdam, Beijing, Brussels, Hamburg, London, Madrid, Milan, Munich, Oslo, Paris, Rome, Shanghai, Singapore, Stockholm and Sydney and Taipei.



**CARDIFF™**  
an Autonomy company

[www.cardiff.com](http://www.cardiff.com)