# Enabling Compliance with 21 CFR Part 11 and EU Annex 11

Ives, J.T., Vahl, S., and Woodward, C.
March 21, 2017

**SUMMARY**

Electronic recordkeeping and data integrity are highly valuable practices within the biopharmaceutical space and tools that enable compliance provide traceability and greater confidence in the results generated. As a tool designed for use by vaccine manufacturers, contract research organizations and government agencies, Cypher One provides compliance opportunities with both USFDA 21 CFR Part 11 and EU Annex 11 guidance.

## Introduction

The Cypher One system has been designed to support compliance with U.S. and European Union requirements for electronic records and electronic signatures. These are often referred to as 21 CFR Part 11 and Annex 11, respectively. This document is organized by listing each requirement and indicating how the Cypher One system enables compliance. Note that compliance implementation relies on the facility to follow good manufacturing practices (GMP) when using the Cypher One. For example, Cypher One supports restricted access by requiring user login, but the facility must ensure that each user's identification and login are unique to be in full compliance.

**21 CFR Part 11 - Section 11.10 Controls for closed systems.**

| Regulation | Cypher One Compliance and Support |
|---|---|
| (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records | Verification and validation protocols testing Cypher One's performance in these areas have been completed as part of the design control process at InDevR, which is certified to ISO 13485:2003.<br>The system provides an electronic audit trail to track actions executed within the Cypher One software.<br>Each facility is responsible for validating that Cypher One meets their user needs. |
| (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. 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 | Electronic and paper records of Cypher One operations are available for export. |

| | |
|---|---|
| (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period | Cypher One supports the user's ability to download records. Long term storage and backup policies are the responsibility of the facility. |
| (d) Limiting system access to authorized individuals | Login is handled by the Windows login system, and Windows' security tools should be used to ensure that only authorized users can login.<br>It is the facility's responsibility to maintain unique login names and passwords for authorized users. |
| (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 | An audit trail preserving operator name, time stamp, associated records, and more information is integral to the Cypher One system. Authorized users have access to the audit trial for review and storage. |
| (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate | NA (Not applicable)<br>The different user interfaces/views of Cypher One address different aspects the operation, but the exact sequence can be variable depending on the user's needs. |
| (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 | Only individuals authorized by the facility should have usernames and passwords, and within those authorized individuals, two levels of user permissions are provided by Cypher One. The capabilities of the two different levels are described in the Cypher One Operation Manual. |
| (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction | The Cypher One software incorporates the serial number/identifier of the associated computer when recording experimental information in the database. |
| (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 | The user facility is responsible. |
| (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 | The user facility is responsible. |

| | |
|---|---|
| (k) Use of appropriate controls over systems documentation including:<br>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance<br>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation | The user facility is responsible for controlling documentation, including laboratory procedures. Customer facing documentation provided by InDevR, such as Cypher One operation manuals, will be clearly marked with revision number and date of release. |

**21 CFR Part 11 - Section 11.50 Signature manifestations.**

| Regulation | Cypher One Compliance and Support |
|---|---|
| (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:<br>(1) The printed name of the signer;<br>(2) The date and time when the signature was executed; and<br>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature | Plate approval requires the logged in and authorized user to affirmatively approve the record. The approval process also includes a comment option where the user can enter the basis for the action. The user's name, date and time of the action, and the comment are saved in the Cypher One database. |
| (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 part of any human readable form of the electronic record (such as electronic display or printout) | Only authorized and logged in users at the appropriate level can approve plates. All database entries are available for display and as printouts for authorized personnel. |

**21 CFR Part 11 - Section 11.70 Signature/record linking.**

| Regulation | Cypher One Compliance and Support |
|---|---|
| (a) 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 | Electronic signatures are directly linked to the associated event in the database. Database access is limited to select personnel as chosen by the facility. |

**Annex 11 - Operational Phase**

| Regulation | Cypher One Compliance |
|---|---|
| 5. Data.<br>Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | The Cypher One system does support import and export of information through comma separated value (CSV) files. The user facility is responsible for ensuring that the transfer is performed accurately. |
| 6. Accuracy Checks.<br>For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management. | The user facility is generally responsible for verifying manually entered information. Cypher One software does require plate approval as an intentional opportunity for data review. |
| 7. Data Storage.<br>7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.<br>7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | The Cypher One system supports printouts and electronic backup, but the user facility is responsible for the associate procedures and maintenance. |
| 8. Printouts.<br>8.1 It should be possible to obtain clear printed copies of electronically stored data.<br>8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry. | Cypher One allows printouts of all records, including plate images.<br>Audit trails can be printed, and any manual override of Cypher One titer calls are automatically recorded. |
| 9. Audit Trails.<br>Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed. | Audit trails can be electronically displayed and printed by authorized personnel. Reasons for changes or other comments can be entered by the user in the Notes field and are preserved in the database. |

| | |
|---|---|
| 10. Change and Configuration Management.<br>Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure. | Users shall be notified by InDevR in the event of future Cypher One revisions. InDevR will perform verification and validation consistent with approved design control procedures, but the user facility is responsible for its own internal validation. |
| 11. Periodic Evaluation.<br>Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports. | The user facility is responsible for ongoing processes. |
| 12. Security.<br>12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.<br>12.2 The extent of security controls depends on the criticality of the computerised system.<br>12.3 Creation, change, and cancellation of access authorisations should be recorded.<br>12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | Login is handled by the Windows login system, and Windows' security tools should be used to ensure that only authorized users can log in.<br>It is the facility's responsibility to maintain unique login names and passwords for authorized users.<br>An audit trail preserving operator name, time stamp, associated record change, and more information is integral to the Cypher One system. Authorized users have access to the audit trial for review and storage. |
| 13. Incident Management.<br>All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions. | The user facility is responsible for root cause investigations, corrective actions, and other GMP processes. |
| 14. Electronic Signature.<br>Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied. | Electronic signatures in the Cypher One system record the user's name, date and time of the action, and an optional comment. This information is directly linked to the associated event and saved in the database. |

| | |
|---|---|
| 15. Batch Release.<br>When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature. | Batch release is not applicable to the Cypher One system, although Plate Approval within the Cypher One system requires positive affirmation by an authorized individual through an electronic signature process. |
| 16. Business Continuity.<br>For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual of alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested. | The user facility is responsible for risk assessments and business continuity plans. |
| 17. Archiving.<br>Data may be archived. This data should be checked for accessibility, readability, and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | Cypher One supports the user's ability to download records. Long term storage and backup policies are the responsibility of the facility. |

**References**

1. Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 Electronic Records: Electronic Signatures.
2. European Commission, Health and Consumers Directorate – General, The Rules Governing Medicinal Products in the European Union, Volume 4 Good Manufacturing Practice, Annex 11: Computerised Systems.