# US FDA 21 CFR Part 11 Support

CyTOF XT PRO system software complies with relevant 21 CFR Part 11 requirements.

## **11.10** Controls for Closed Systems

CyTOF™ Software with 21 CFR Part 11 Module is a closed system utilizing either Windows domain authentication or user accounts with strong expiring passwords for digital signatures. User authentication is required for starting software and for software operations that affect creating data records.

| Section | Requirement | Compliance |
|---|---|---|
| 11.10a | Validation to ensure accuracy, reliability and consistent intended performance, and the ability to discern invalid or altered records. | CyTOF XT PRO system development was performed under ISO 13485-compliant medical device standards for RUO. Data record files are retained per the user's laboratory policies. CyTOF Software retains all generated data file SHA-256 hashes and provides checksum verification functions to discern altered data files. Audit log verification is performed in software to ensure no alterations to audit logs have occurred. IQ and OQ procedures are available for system validation. Generated data record files are retained per the user's laboratory policies. |
| 11.10b | Generate accurate and complete copies of records in both human-readable and electronic form suitable for inspection, review and copying by the agency. | The CyTOF XT PRO system generates flow cytometry standard (FCS) data files and human-readable PDF files per processed sample and saves each to a user-specified file folder. All data files exported from the system are cryptographically hashed with the SHA-256 algorithm and retained for file verification. Additionally, a hash manifest file is exported for data transfer verification. Once files have been generated, users must follow appropriate steps to ensure protection of records in accordance with the laboratory's practices. |
| 11.10c | Provide protection of records to enable their accurate and ready retrieval throughout the record retention period. | CyTOF XT PRO generates data files, which are not retained in system databases, but are retained in accordance with the laboratory's file management practices. Records retained in the system require appropriate permissions for modification or deletion. |
| 11.10d | Limit system access to authorized individuals. | CyTOF Software requires a user login with password. Software operations that generate or alter data records require an authorized user, with appropriate permissions, to provide reason and authentication. User access and operation permissions are managed by system administrators. The CyTOF XT PRO system supports Windows domain authentication user accounts and/or CyTOF user accounts with strong passwords and required expiration. |
| 11.10e | Maintain audit trails to record the date and time of operator entries and actions that create, modify or delete electronic records. Retain audit trail documentation for at least the time required for the subject electronic records and ensure the documentation is available for agency review and copying. Changes shall not obscure previous information. | CyTOF Software generates time-stamped audit logs associated to the experiments that generate the sample records. Audit logs are stored in an independent database and retained in accordance with laboratory data management practices. Audit logs are verified automatically in the user interface to ensure no modification has occurred. Audit logs can be reviewed or exported but not altered through the software. |
| 11.10f | Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | CyTOF Software restricts operations based on the state of the instrument and the permissions assigned to the operating user. |

| | | |
|---|---|---|
| 11.10g | Use of authority checks to ensure that only authorized individuals can use the system. | CyTOF Software performs a challenge response for user interactions to generate or alter the generation of records. This challenge response requires the user to provide a reason and valid user credentials to perform the action. |
| 11.10h | Use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction. | CyTOF Software has input verification for individual data fields, which are available for modification by the user. Error messages and validation ranges are provided. File checksum verification functions are also provided to ensure record integrity. |
| 11.10i | Confirm that the system can determine if individuals who develop, maintain or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks. | Standard BioTools provides user training and documentation for operation of the system and software. It is the responsibility of the user's organization to ensure training of staff. |
| 11.10j | Establish written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, to deter record and signature falsification. | This is the responsibility of the user's organization. |
| 11.10k(1) | Provide adequate controls over the distribution of, access to and use of documentation for system operation and maintenance. | CyTOF Software has a user guide available to all users. The user guide is updated appropriately with system software updates. All updates are made available to end users to ensure optimal system operation through the field support organization. |
| 11.10k(2) | Revise control procedures to maintain an audit trail that documents time-sequenced development and modification of system documentation. | CyTOF Software has a user guide available to all users. The user guide is updated appropriately with system software updates. All updates are made available to end users to ensure optimal system operation through the field support organization. |

## **11.30** Controls for Open Systems

| Section | Requirement | Compliance |
|---|---|---|
| 11.30 | In conjunction with the use of open systems to create, modify, maintain or transmit electronic records, 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. | CyTOF Software operates as a closed system. This is not applicable. |

## **11.50** Signature Manifestation

| Section | Requirement | Compliance |
|---|---|---|
| 11.50a | Ensure signed electronic records contain the printed name of the signer, the date and time the signature was executed, and the meaning associated with the signature. | Audit-traced records within the software contain the username of the signer, the date and time of the signing, and the reason. |
| 11.50b | Ensure that the following are subject to the same controls as electronic records and that they are part of any human readable form of the electronic record: the printed name of the signer, the date and time the signature was executed, and the meaning associated with the signature. | The signing username, reason, and date and time of the record are displayed in the interface and included in the FCS metadata for each data record generated per sample. |

## **11.70** Signature/Record Linking

| Section | Requirement | Compliance |
|---|---|---|
| 11.70 | Electronic and handwritten signatures executed to electronic records link 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. | CyTOF Software maintains audit log records, including signed actions, which are linked to the executing records from which they originate. CyTOF Software automatically verifies the integrity of the audit log and alerts the user if the record audit log, including signatures, has been modified from its creation. |

## **11.100** Electronic Signatures

| Section | Requirement | Compliance |
|---|---|---|
| 11.100a | Electronic signatures are unique to one individual and shall not be reused by, or reassigned to, anyone else. | CyTOF Software ensures that every combination of username and password is unique to the user. If the username is disabled, it cannot be reused for other users. It is the responsibility of the user's organization to verify the identity of all users. |
| 11.100b | Verification of individual identity before an electronic signature, or any element of such electronic signature, has been established, assigned, certified or otherwise sanctioned to that individual. | This is the responsibility of the user's organization. |
| 11.100c | Company certifies to the agency, prior to or at the time of such use, that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures. | This is the responsibility of the user's organization. |

## **11.200** Electronic Signature Components and Controls

| Section | Requirement | Compliance |
|---|---|---|
| 11.200a | Maintain at least two distinct identification components such as an identification code and password, to be used only by their genuine owners. | CyTOF Software challenge/response interface is required to be authenticated by a user with appropriate permissions for the required action. The user must specify their username and password for this action to be performed. This authorization action is retained in the audit log for the record as the digital signature along with timestamp and username. |
| 11.200b | Electronic signatures based upon biometrics cannot be used by anyone other than their genuine owner. | CyTOF Software does not support biometric electronic signatures. |

## **11.300** Controls for Identification Codes/Passwords

CyTOF Software supports two models of user authentication to allow for mixed-use environments: (1) Windows authentication can be utilized and it is the responsibility of the laboratory to ensure compliance, and (2) CyTOF authentication (username/password) is also available and is the responsibility of the laboratory administrator with appropriate permissions to configure and ensure compliance.

| Section | Requirement | Compliance |
|---|---|---|
| 11.300a | Maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. | (a) Windows authentication: The laboratory is responsible for compliance with user account setup. CyTOF authentication: No two user accounts can have the same combination of username and password. The combinations of username and password must be unique. |
| 11.300b | Ensure that identification code and password issuances are periodically checked, recalled or revised (for example, to cover such events as password aging). | Windows authentication: The laboratory is responsible for compliance with user account setup. CyTOF authentication: Password expiration is set by administration and applied when a user changes their password. |
| 11.300c | Electronically de-authorize 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. | Windows authentication: The laboratory is responsible for compliance with user account setup. CyTOF authentication: Password expiration is set by administration and applied when a user changes their password. |
| 11.300d | 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. | Windows authentication: The laboratory is responsible for compliance with user account setup. CyTOF authentication: An audit trail logs successful and failed login attempts. |
| 11.300e | Employ 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. | Periodic checks are the responsibility of the user. |