FDA 21 CFR Part 11 Compliance

Bluechiip Stream™ Sample Manager Software

Bluechiip Limited confirms its product, Bluechiip Stream™ Sample Manager v5.6.0 has been developed using the highest possible design and coding standards managed by Bluechiip's ISO9001 certified Quality Management Systems and in accordance with the FDA General Principles of Software Validation (January 2002). Bluechiip's formal in-house development and testing ensures that the software program performs in a manner consistent with the approved functional specifications for this version. When configured suitably and with appropriate organizational controls, the system ensures the integrity of data, preventing unauthorized users from logging into the system to create and/or modify electronic records.

Signed 

Scott Turner, Engineering Manager

Date 12 Nov 2021

The checklist provided describes how the Bluechiip system currently provides support for electronic records.

No.	21 CFR Part 11 Clause	Bluechiip Comment	Compliant
11.10a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The system has the ability to be validated, within the bounds of system scope. As part of inherently being able to use the system, the user has the ability to challenge functions appropriate to the needs of the organization. Electronic records can be created and maintained.	Yes
11.10b	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.	Copies of records can be downloaded in both human readable and electronic format. Reporting tools allow users to generate both electronic and print-friendly human readable copies of samples, user activity, tasks, event logs and audit trail.	Yes
11.10c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Electronic records are not deleted from the system and audit trails are maintained for changes to records. Copies of records can be downloaded in both human readable and electronic format. The retention period is limited by the storage capacity of the Bluecube. The system warns users when storage is almost full.	Yes
11.10d	Limiting system access to authorized individuals.	Only authorized persons have access to the system including both Stream Software and the readers. The system maintains access control using usernames, passwords, key fobs and pins and can be configured to enforce 2-factor authentication. Key fobs cannot be used within the system until attributed to a user. Operational controls exist for user activation and password reset.	Yes
11.10e	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.	Audit trails are maintained for changes to electronic records. Audit records are stored on the Bluecube and cannot be altered. Like all electronic records, the retention period is limited by the storage capacity of the Bluecube. The system warns users when storage is almost full.	Yes
11.10f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational controls do exist for routine operations to preserve system workflows including: - User onboarding - Password reset - Registering and accessioning samples - Tasks Bluechiip advises users to determine whether the operational controls of the system are suitable for their needs.	User to comply
11.10g	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.	The system only grants access to authorized users. The level of access to is defined and controlled within the system for role-based tasks (administrator and user). The system does not currently support 21 CFR Part 11 requirements for electronic signatures.	Yes
11.10h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The system is designed to accept data from authorized users and system specific readers, MEMS chips and barcodes. The system is designed to only accept data input from Bluechiip readers once they are configured to the system by an authorized user. Controls exist for checking the uniqueness of barcodes used for identification purposes prior to being registered in the system and upon editing. Information on external barcodes that can be accepted by the scanners can be found in the Bluechiip User Manual.	Yes

11.10i	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Customers must determine the competencies and training requirements of persons using the system. Only trained users should be allowed to use the system. The system is designed to prevent access to unauthorized users. The system does not currently support electronic signatures.	Yes
11.10j	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.	Users should not share passwords, pin numbers and fobs. Users should create their own password when activating their user account and follow organizational IT security policies where applicable. The system does not currently support electronic signatures.	Yes
11.10k	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.	User Manuals are controlled documents maintained under Bluechiip's Quality Management System. Each User Manual references which instruments and software version number it is applicable to.	Yes
11.30	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 signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	The system is considered to be a closed system	n/a

Note: The system does not currently support electronic signatures.

Bluechiip Limited
info@bluechiip.com