US FDA 21 CFR Part 11 Support: CGX10 Software

CGX10 Software (version 1.0 or later) when used in the Operator (OP) mode enables compliance with 21 CFR Part 11 guidelines as described in the following table.

Section	Requirement	Compliance
11.10	**Controls for Closed Systems** Persons 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. Such procedures and controls shall include the following:	
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The CGX10 system software is released following validation and verification testing conducted by Sony. The validity of the exported Sort Report data is ensured by checksum, and the raw data and audit log cannot be tampered with. In addition, IQ and OQ procedures for installation qualification and operational qualification of the CGX10 system are available from Sony.
11.10(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.	The CGX10 system software provides both electronic and human-readable formats of the records (Sort Reports) in the system database. The reports can be archived on a USB flash drive or network and retrieved outside the device. Reports archived outside the equipment can be printed for inspection, offline review, and FDA reproduction. Once reports are archived outside the device, users must take needed steps to ensure protection of data and records.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The CGX10 system software secures files, data files, and result information in an encrypted format within a hidden folder structure controlled by an indexing database. All records are retained until a user with appropriate privileges decides to delete records. Records that have not been archived cannot be deleted. The validity of any exported/imported data is ensured by checksum. All metadata is maintained in the database and is not available through the Windows file system. Users must manage records that are archived from the software according to prevailing policies and processes to ensure data protection.
11.10(d)	Limiting system access to authorized individuals.	The CGX10 system software requires a password for all users when logging in. Each user has a defined role, including access privileges. Roles are assigned within the User Management function in the Administrator menu. Only active users may log in and access the software with a valid user ID and password. Users and their roles should be managed in an administrative ledger or similar document in addition to with the functions available within the software.
11.10(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.	The CGX10 system software automatically generates a secure, time-stamped audit trail of all user actions that affect the Sort Report, including date and time, and user IDs. Users cannot modify, delete, or deactivate the audit trail. The audit trail is maintained within the CGX10 system software and can also be exported for review. The date and time can be changed only by a user with an administrator privilege, and date and time settings and changes also are recorded in the audit trail.

Section	Requirement	Compliance
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The CGX10 system software restricts what users can do based on the state of the system and the permissions associated with the logged-in user's account (e.g., Administrator, Operator, Process Developer).
11.10(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.	The CGX10 system software is accessed using a valid user ID and password. Based on the role and privileges associated with the logged-in user's account, the software provides the user with the authority to carry out particular functions. These privileges include tasks such as electronic signature application to a Sort Report, deletion of record, and archiving of a Sort Report.
11.10(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The CGX10 system software has been designed with limitations related to fields of information, and it includes an error management/messaging capability that informs the user when invalid information is input into a software field. The CGX10 system software also confirms the validity of the Sort Report by attaching a checksum value to it. The checksum value is attached to the Sort Report when it is exported. Before a Sort Report can be imported, the software checks the checksum value and restricts the import if the value has changed since creation/export.
11.10(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.	Sony provides user training and documentation for operation of the CGX10 system and software. The user's organization is responsible for ensuring training of staff and providing needed information on the Electronic Record/Electronic Signature operating procedure based on their own policies and procedures.
11.10(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.	Written policies holding individuals accountable for actions are the responsibility of the user's organization. However, password policies (expiration time and number of unsuccessful login attempts) can be configured by an Administrator according to the standard operating procedures of the organization. In addition, password length, complexity, and restrictions on reuse are implemented by the system.
11.10(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.	The CGX10 system documentation is updated as needed based on the change control process under the Quality Management System. The field support organization makes all updates available to end users to ensure optimal system operation.
	(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Updates to system documentation included in the CGX10 system software are recorded in the audit trail. Management of documentation provided outside the CGX10 system software is the responsibility of the user's organization.
11.30	**Controls for Open Systems**	
	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.	Not applicable. The CGX10 operates as a closed system.

Section	Requirement	Compliance
11.50	**Signature Manifestations**	
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (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.	The CGX10 system software requires signature of electronic records (Sort Report). Upon signature, the Sort Report will include the following: 1) The printed name of the signer. 2) The date and time the signature was executed. 3) The meaning associated with the signature. The signature granted by the CGX10 system software indicates that the Sort Operation has been completed, aborted, or failed, and does not necessarily mean approval. If an approval signature is required for Sort Reports archived outside the system, the signature is the responsibility of the user's organization.
11.50(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).	All electronic records within the CGX10 system software are date and time stamped, signed by the author, and provided in a human-readable format in the PDF Sort Report. Checksums are available to detect modifications of signed Sort Reports.
11.70	**Signature/Record Linking**	
	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.	The CGX10 system software creates Sort Reports in PDF format, and electronic signatures are granted using PDF functionality. The PDF function ensures that electronic signatures cannot be reused.
11.100	**General Requirements**	
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The CGX10 system software provides a unique user ID and password to each user. If the user ID is disabled, it cannot be reused for other users.
11.100(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.	It is the responsibility of the user's organization to verify the identity of all users of the system.
11.100(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.	This is the responsibility of the user's organization.
	(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.	This is the responsibility of the user's organization.
11.200	**Electronic Signature Components and Controls**	
11.200(a)	(1) Employ at least two distinct identification components such as an identification code and password.	A software requires a unique user ID and password to apply an electronic signature. Both components are necessary for each signing, separately from login.
	(ii) 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.	The CGX10 system software requires both components at every signing, separately from login.

Section	Requirement	Compliance
	(2) Be used only by their genuine owners; and	The CGX10 system software ensures the user ID and password are unique. It is the responsibility of the user's organization to ensure the user ID and password are kept secure to avoid misuse by anyone other than the genuine owner.
	(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.	The CGX10 system software ensures that only a user with the administrator privilege and the user themselves can change a password.
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	The instrument does not support biometric signatures.
11.300	**Controls for Identification Codes/Passwords** 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:	
11.300(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.	No two individuals can have the same combination of ID and password. User IDs and passwords must be unique.
11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Passwords are set to expire when they are first created or reset. The password expiration can be enabled or disabled by the administrator. To comply with Part 11, the user's organization should enable and set password expiration.
11.300(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.	Administrators can delete accounts or change compromised passwords as needed. If a user password is reset by an administrator, the reset password is for temporary use and must be changed at first login.
11.300(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.	After a specified number of consecutive failed login attempts, the software locks out the problematic user. The specified number of times can be set by the administrator to suit the operation of the user's organization.
11.300(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.	Periodic checks are the responsibility of the user's organization. Administrators are encouraged to periodically check for access restrictions and unauthorized data manipulation.

The CGX10 Cell Isolation System and related products are intended for use by trained laboratory technicians in research, process development or manufacturing environments all related to Advanced Therapy Medicinal Products (ATMP) or regenerative medicine, including cell and gene therapy. The CGX10 instrument and related products are for ex vivo cell separation processing only, and are not intended for therapeutic, diagnostic, or human in vivo applications. Any clinical application of the cells is exclusively within the responsibility of the user of the CGX10instrument and related products. For the manufacturing and use of cells in humans, regulations must be followed. The CGX10 Cell Isolation System and related products are not sold as medical devices.

11.13.022223.0