eppendorf

WHITE PAPER No. 010 I Juli 2023

Implementation of 21 CFR Part 11 and EU GMP Annex 11 in the epMotion® Software.

Electronic records and electronic signatures in the regulated environment of the pharmaceutical and medical device industries.

Executive summary

The pharmaceutical, healthcare, and medical device industries, along with related fields, must carefully consider regulatory obligations. The U.S. Food and Drug Administration (FDA) implemented the 21 CFR Part 11 guideline to regulate electronic records and signatures, while the European Unions's EudraLex issued Annex 11 to govern computerized systems in industries producing medicinal products.
This white paper conducts a comparison between the legal requirements of both 21 CFR Part 11 and EU GMP Annex 11 and the technical specifications of the "Enhanced Feature Set GxP" for the epBlue software (epBlue GxP), used in conjunction with the epMotion automated liquid handling device, in the following referred as the "the system".
In conclusion, the epBlue GxP software assists customers in achieving compliance with both 21 CFR Part 11 and EU GMP Annex 11.

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
Sec. 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:	The system supports users in fulfilling these requriements:

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Eppendorf SE, as the supplier of the epBlue GxP software maintains a quality management system ensuring compliance with the relevant requirements of both ISO 13485 and ISO 9001 for quality management systems. The performance of the software was verified through tests that assessed accuracy, reliability, and consistent performance. Additionally, the software has the capability to checksum files in order to detect any invalid or altered files. While it is the responsibility of the user organization to validate their application in accordance with regulatory expectations, Eppendorf SE offers services to support the user in the validation process. These services include system installation qualification (IQ) and operational qualification (OQ).
(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 epBlue GxP software creates various types of electronic records, such as applications, application log files, and an audit trail. To enable long-term archiving of these records, the software uses the PDF format. The records can be viewed in the epBlue GxP software or any other PDF display program in a human-readable format on a screen or printer and support users batch records.
8. Printouts	
8.1 It should be possible to obtain clear printed copies of electronically stored data.	To confirm that the data was generated by the the system, a master certificate is provided for the PDF viewer software. However, it is the responsibility of the user organization to maintain the authenticity and integrity of the printed records.
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.	

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The epBlue GxP software supports protection of records in the following ways:
17. Archiving **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.**	> All records are stored in an industry standard database. > Data integrity of files is ensured via checksum. > Database backup function. > Archiving and export of records as signed PDF files.
7. Data storage **7.1 Stored data should be secure and accessible throughout the retention period.** **7.2 Possibility to perform regular back-ups.**	It is the responsibility of the user organization to define retention periods and that data is checked during the archival period for accessibility, readability, and accuracy.
(d) Limiting system access to authorized individuals. **12. Security** **12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons.**	The epBlue GxP software provides its own user management and supports role-based security configurations to control access to authorized individuals only. Implementing a system for password protection should be the obligation of the user organization.
(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. **14. c. Electronic Signature - Do electronic signatures include the time and date that they were applied?** **12.4 Security - 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.** **9. Audit trails** **Consideration of audit trail generated by the system.**	The epBlue GxP software generates a continuous audit trail automatically, which captures the time stamp and user name of all actions taken on electronic records (such as signing, creating new revisions and archiving). The audit trail is shielded from any attempts at manipulation by both administrators and users. The system also includes revision control for user-modifiable records, such as applications. Records are never permanently deleted or overwritten, and all revisions can be accessed and exported from the system at any given time. The audit trail can be exported and saved outside the system.

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. **6. Accuracy Checks** **Possibility for additional check on the accuracy of data by a second operator or by validated electronic means.**	The epBlue GxP software enables administrators to configure the process of signing records, e.g. how many signatures by which users and in which sequence are necessary for a record to be authorized.
(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. **12. Security** **12.2 The extent of security controls depends on the criticality of the computerized system.**	The administrator can assign user rights incl. signature rights. This ensures that only authorized users can electronically sign a record. The system does not support physical controls like keys, pass cards or biometrics.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. **5. Data** **Appropriate built-in checks for electronically exchanged data with other system should exist.**	The epBlue GxP software comes equipped with built-in features that are specifically intended to verify the system configuration. However, it is the responsibility of the user organization to define procedures for changes on the system configuration. Checksums are used to validate files that are exchanged between the epBlue GxP software and other programs. This functionality helps users to identify errors that may arise during data transfer or manipulation. If an invalid checksum is detected, a warning message will appear to notify the user.
(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. **2. Personnel** **The personnel is qualified to use the system.**	Eppendorf SE has obtained ISO 9001 and ISO 13485 certification for the development, production, distribution, sales, and service of automated pipetting systems. As a result, the company provides regular trainings to its employees in the aforementioned areas to ensure their proficiency. Additionally, Eppendorf SE provides system training to educate users on the proper operation of the system.
(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.	It is the responsibility of both users and system administrators to carry out electronic signatures in accordance with applicable laws, just as they would with handwritten signatures.

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
(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. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Documentation for system operation and maintenance including version numbering is supplied with each version of the system. All changes are subject to a defined change control and documentation process. The epBlue GxP software comes equipped with built-in features that are specifically intended to verify the system configuration. The audit trail captures changes made to the system. However, it is the responsibility of the user organization to define procedures for changes on the system configuration.
Sec. 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.	The epMotion/epBlue GxP system is a closed system. The system supports users in ensuring authenticity and integrity by embedding a digital signature in records exported as PDF files. The signature can be verified using standard software like Adobe Reader. Checksums are used to compare files exchanged between epBlue GxP and other programs.
Sec. 11.50 Signature manifestations.	
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. (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).	Electronic records that have been signed within the system contain the following details: 1. The printed name of the signer. 2. The date and time at which the signature was executed. 3. The significance or intent associated with the signature. Upon being signed, electronic records are classified under one of three states, namely “created,” “reviewed,” or “authorized,” depending on the signer’s role and the number of signatures involved. The system also ensures the same level of control over the information related to electronic signatures by encrypting it and storing it within the record. This information can be easily viewed in human-readable form within both the electronic record and any printed copies.

21 CFR Part 11 / EU GMP Annex 11 requirements	Implementation in epBlue GxP
Sec. 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. **14. Electronic Signature** **14. b. Electronic signatures are expected to be permanently linked to their respective record.**	The epBlue GxP software produces digital signatures using the standardized Digital Signature Algorithm procedure. The system's electronic signatures are permanently embedded into the document and cannot be altered, replaced, or deleted.
Subpart C – Electronic Signatures	
Sec. 11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The epBlue GxP software guarantees that usernames are unique and cannot be reused once a user account has been deleted. However, it is the responsibility of the user organization to establish security policies that will prevent user account duplication and deletion.
(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.	This is a responsibiltiy of the user organization and should be defined in a user Standard Operation Procedure (SOP).
(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. (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. **14. Electronic Signature** **14 a. Electronic signatures are expected to have the same impact as hand-written signatures within the boundaries of the company.**	This is a responsibility of the user organization to manage this certification to the agency.

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
Sec. 11.200 Electronic signature components and controls.	
a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (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 all of the electronic signature components.	The system requires identification by user name and password. The system always requires both user name and password to execute a signature.
(2) Be used only by their genuine owners; and	The system forces the password to be entered each time a signature is exercised. It is the responsibility of the user organization to define SOP concerning logical security.
(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 customer bears the responsibility for safeguarding Administrator access to the system and ensuring that system administration tasks are carried out by reliable personnel. To ensure secure management of the system, the customer is encouraged to create regulations (e.g. via a SOP) mandating that the affected user must be present when an administrator modifies or resets their password.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable. The system does not support biometric identification.
Sec. 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:	
(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.	The epBlue GxP software ensures that user names are unique. Once a user account is deleted, it is not possible to create a new user account with the same name.

21 CFR Part 11 / **EU GMP Annex 11** requirements	Implementation in epBlue GxP
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The epBlue GxP software enables administrators to define periods of validity for passwords and user accounts. Passwords must consist of a minimum of eight characters and include at least one uppercase letter, one lowercase letter, one number, and one special character. The epBlue GxP software keeps records of the last ten passwords used and requires new passwords to be distinct from those previously used.
(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 have the ability to secure user accounts from unauthorized access by locking them with the epBlue GxP software. In addition, administrators are authorized to reset user passwords. Changes to user accounts are saved in the audit trail.
12. Security **12.3 Creation, change, and cancellation of access authorisations should be recorded.**	The system does not support the usage of tokens, cards, or other similar devices.
(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.	System administrators can define after which period of inactivity the system will be automatically locked and the maximum number of login retries. The epBlue GxP software automatically displays the timestamp of a user's last login.
(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.	epBlue GxP software does not support using tokens, cards and similar devices. The customer is obligated to ensure the proper and safe functioning of the system components and to ensure that no unauthorized changes are made to the system.

EU GMP Annex 11 requirements which do not have a equivalent to 21 CFR Part 11.

EU GMP Annex 11 requirements	Implementation in epBlue GxP
1. Risk Management **Risk management should be applied throughout the life-cycle of the computerised system.**	Risk assessment of computerised system is the responsibility of the user organization.
3. Suppliers and Service Providers **Manufacturer and third parties must have formal agreements in place. The decision to conduct a supplier audit should depend on a risk assessment. The regulated user should examine the documentation provided with off-the-shelf products. If requested, inspectors should have access to relevant audit information.**	Eppendorf SE, as a service provider, is willing to establish written agreements with its customers. Along with the products, Eppendorf SE provides documentation (excluding intellectual property documentation) that is intended to be adequate for assisting customers in using the products in regulated environments. The responsibility of assessing the need for an audit, reviewing product documenation, and providing documentation to inspectors lies with the user organization.
4. Validation **> The validation documentation and reports should cover the relevant steps of the life cycle.** **> Validation documenation should include change control and reports on any deviations.** **> An up to date listing of all relevant systems should be available.** **> User requirement specification should describe the required functions of the computerized system.** **> The regulated user should ensure that the system has been developed in accordance with an appropriate quality management system.** **> A process should be in place that ensures formal assessment of quality and performance measures.** **> If data are transferred to another data format or system, validation should include checks that data are not altered.**	The user organization is responsible for carrying out application validation in line with regulatory expectations and verifying whether the system specifications meet user requirements. The system (and related services) is equipped with features to assisst customers in the validation process. These features include, but are not limited to: > Services such as Installation (IQ) and Operational Qualification (OQ). > Built-in features specifically intended to validate the system configuration. > Checksums used to compare files exchanged between epBlue GxP and other programs. This functionality helps users identify any errors that may occur during data transfer or manipulation. If an invalid checksum is detected, a warning message will appear to notify the user. The provided product specifications and documentation are intended to support the customer in validation and monitoring throughout the system lifecycle. It is the responsiblity of the user organization to implement procedures for changes to computerized systems.
10. Change and Configuration Management **Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.**	It is the responsiblity of the user organization to implement procedures for changes to computerized systems.

EU GMP Annex 11 requirements	Implementation in epBlue GxP
11. Periodic evaluation **Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.**	It is the responsibility of the user organization to perform periodic evalualation of the system.
13. Incident Management **All incidents, not only system failures and data errors, should be reported and assessed.**	The user organization bears the responsibility of establishing an incident management system. The epBlue GxP audit trail assists the user by documenting system failures and errors.
15. Batch release **The system should allow only Qualified Persons to certify the release of the batches and should clearly identify and record the person releasing or certifying the batches.**	The epBlue GxP software allows the export of signed records for print-outs to support users with batch releases.
16. Business Continuity **Provisions should be made to ensure continuity of support for critical processes in the event of a system breakdown.**	It is the customer responsibility to apply appropriate measures to ensure business continuity.

*Requirement text was partially summarized and thus does not correspond to the original text of 21 CFR Part 11 and EU GMP Annex 11.

Your local distributor: www.eppendorf.com/contact
Eppendorf SE · Barkhausenweg 1 · 22331 Hamburg · Germany
eppendorf@eppendorf.com · www.eppendorf.com

www.eppendorf.com