Implementation of 21 CFR Part 11 in the epMotion® Software

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

Preamble

The introduction of electronic signatures in the pharmaceutical, healthcare and medical device industries as well as in related industries requires detailed consideration of the boundary conditions stipulated by American law. Regulations in Europe are in preparation and will be published soon, e.g. EU GMP Annex 11 Computerised Systems.

This White Paper compares the legal requirements of 21 CFR Part 11 with the technical specifications of the hardware and software product epMotion® in combination with the epBlue GxP software, which is being referred to as “the system” in the following.

21 CFR Part 11 Requirement

Sec.11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

Implementation in the system

This document describes the technical implementation and, where applicable, the process-related implementation by work instructions or company policies of the requirements stipulated in the legal text of 21 CFR Part 11 regarding the equivalence of a legally binding signature in electronic form in comparison to a traditional signature executed on paper.

The system creates and maintains the following electronic records:
> applications (definition of worktable equipment and work procedure)
> application logs (detailed record of individual application runs, optionally including sample ID tracking)
> audit trails (detailed chronological record of relevant user and system actions)
21 CFR Part 11 Requirement

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

Implementation in the system

Electronic signatures executed in epBlue GxP meet all the requirements set forth in 21 CFR Part 11. The agency will consider documents signed in this way to be legally equivalent to traditional handwritten signatures.

Electronic records signed with the epMotion software may be used in lieu of paper records, thus improving the workflow.

The hardware and software used to create the electronic signature are made commercially available by Eppendorf and the system documentation is made available for inspection on request.

Sec. 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

The system provides means to create, digitally sign, and maintain electronic records in compliance with this part. The electronic records provide a complete and traceable documentation of all actions performed on the system.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

1. The requirements of this part are met; and

2. The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.
### 21 CFR Part 11 Requirement

#### Implementation in the system

<table>
<thead>
<tr>
<th>Sec. 11.3 Definitions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.</td>
<td></td>
</tr>
<tr>
<td>(b) The following definitions of terms also apply to this part:</td>
<td>The system does not make provision for biometrics. Typing of user ID and password are used for identification.</td>
</tr>
<tr>
<td>(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).</td>
<td>The system is configured as a closed system and meets these requirements. Access to the system is configured by its user management feature. All data are held in an industry standard database that is only accessible through the system’s software. The system can operate in corporate networks only for data exchange processes.</td>
</tr>
<tr>
<td>(2) Agency means the Food and Drug Administration.</td>
<td>The system uses a digital signature which employs cryptographic methods to verify the identity of the signer. This allows the identity of the signer and the integrity of data to be recognized.</td>
</tr>
<tr>
<td>(3) Biometrics means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.</td>
<td>All electronic records defined here can be saved and retrieved in accordance with agency and legal requirements through the use of electronic signatures. The PDF format is used for long-term archiving.</td>
</tr>
<tr>
<td>(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.</td>
<td>The system stores electronic signatures in its database with the records that have been signed. When exporting electronic records as PDF files, the electronic signatures are embedded as encrypted code that can be verified with appropriate software (such as Adobe Reader).</td>
</tr>
<tr>
<td>(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.</td>
<td></td>
</tr>
<tr>
<td>(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.</td>
<td></td>
</tr>
<tr>
<td>(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.</td>
<td></td>
</tr>
</tbody>
</table>
21 CFR Part 11 Requirement

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Implementation in the system

The system does not make provision for handwritten signatures. Electronic handwritten signature capture devices are not supported. However, all records can be printed and manually signed on paper.

The system is designed as a closed system.

Subpart B – Electronic Records

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:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

The system supports users and agencies in fulfilling these requirements by the following ways:

The system has been audited to comply with the relevant requirements of:
> ISO 62304 Class B
  (Medical device software – software life cycle processes)
> 21 CFR § 820 (Quality system regulation)
> GAMP5 Categories 3 and 4 and supports validation according to these requirements.

The system is supplied with the appropriate certificates of conformity.

(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 agency can use the system software, as well as any other PDF display programs, to view the audit-proof data in human readable form on a screen or a printer. A master certificate is provided for PDF viewer software to verify and check whether the data was generated by the system. The FDA explicitly stipulates the use of PDF for long-term archiving.
21 CFR Part 11 Requirement

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(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.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(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.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(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.

(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.

Implementation in the system

The system ensures protection of records in the following ways:
> All records are stored in an industry standard database
> Data integrity of the records is ensured via checksum.
> Database backup function
> Archiving and export of records as signed PDF files

The system provides its own user management, allowing the assignment of user rights to limit access to authorized individuals only. Password protection is enforced.

The system automatically creates a continuous audit trail containing the time stamp and user name of all actions performed (like signing, creating new revisions, archiving, etc.) on electronic records. The audit trail is protected from manipulation by administrators or users.

The system provides revision control for user modifiable records (applications). Records are never permanently deleted or overwritten. All revisions can be viewed and exported from the system at any time.

The system 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.

The administrator can assign user rights incl. signature rights. This ensures that only authorized users can electronically sign a record.

The system is delivered as a completely manufacturer qualified and documented package. Service and maintenance agreements for re-qualification can be concluded.

The hardware and software developers of the system are certified for the necessary qualifications.

Users and system administrators must receive training (provided by Eppendorf) to ensure correct system operation in accordance with legal requirements.

Users and system administrators must receive appropriate legal training and shall be obligated by signature to execute electronic signatures in compliance with the applicable laws analog to handwritten signatures. It is recommended to document this e.g. in an SOP (Standard Operating Procedure).
21 CFR Part 11 Requirement

(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.

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.

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).

Implementation in the system

Each version of the system is supplied with the relevant system information provided with version numbering. All changes are subject to a defined change control and documentation process. In addition, the system can record changes made to its components.

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.

The system enforces the same control for the information associated with electronic signatures by encrypted storage in the record. This information can be displayed in human readable form in the electronic record and the printout.
21 CFR Part 11 Requirement

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.

The electronic signatures generated by the system are saved as inseparably embedded into the document. This prevents copying and disclosure of signatures, as well as falsification of electronic records.

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.

(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.

The customer is instructed to verify the identity of all persons who are authorized to execute an electronic signature.

(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.

The customer is instructed to certify to the agency (FDA) that electronic signatures are the legally binding equivalent of traditional handwritten signatures with the following wording: “Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are 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.
21 CFR Part 11 Requirement

Sec. 11.200 Electronic signature components and controls.

<table>
<thead>
<tr>
<th>a) Electronic signatures that are not based upon biometrics shall:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Employ at least two distinct identification components such as an identification code and password.</td>
</tr>
<tr>
<td>(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.</td>
</tr>
<tr>
<td>(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</td>
</tr>
<tr>
<td>(2) Be used only by their genuine owners; and</td>
</tr>
<tr>
<td>(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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implementation in the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>The system requires identification by user name and password.</td>
</tr>
<tr>
<td>The system always requires both user name and password to execute a signature.</td>
</tr>
<tr>
<td>The system enforces password complexity policies.</td>
</tr>
<tr>
<td>It is in the customer’s responsibility to ensure that the Administrator access to the system is protected and that the system’s administration is performed by trustable persons. The customer is advised to establish rules (e.g. through an SOP), that the affected user has to be present while an administrator changes or resets his or her password.</td>
</tr>
<tr>
<td>The system does not support biometric identification.</td>
</tr>
</tbody>
</table>

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
21 CFR Part 11 Requirement

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.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(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.

(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.

(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.

Implementation in the system

The system ensures that user names are unique.

The system enables administrators to define periods of validity for passwords and user accounts.

The system enables administrators to lock user accounts to prevent use of compromised credentials. Administrators also can reset user passwords.

The system does not support using tokens, cards and similar devices.

A user account is automatically locked after three unsuccessful login attempts.

The system automatically displays the timestamp of a user’s last login.

The system does not support using tokens, cards and similar devices.

The user is advised to make sure that the system’s computer is kept clean of any software programs that may be used to intercept input of user names and passwords. This may be accomplished by limiting access rights and using appropriate anti-virus software.