

JMobile support for FDA 21 CFR 11

This document describes the functions available in JMobile V2.0 SP1 for compliance with the requirements of FDA 21 CFR Part 11.

Copyright © 2016 Exor International S.p.A. – Verona, Italy

Subject to change without notice

The information contained in this document is provided for informational purposes only. While efforts were made to verify the accuracy of the information contained in this documentation, it is provided “as is” without warranty of any kind.

Third-party brands and names are the property of their respective owners.

www.exorint.net

Contents

1 JMobile conformity with FDA 21 CFR Part 11..... 4

1 JMobile conformity with FDA 21 CFR Part 11

JMobile includes a set of functions for responding to the requirements specified in FDA 21 CFR Part 11.

The standard is intended to provide a solution for securely handling electronic records and electronic signatures in industrial applications.

The table lists all the requirements specified by the regulation and reports the functions available in JMobile for compliance.

The content is updated to JMobile V2.0 SP1.

Chapter	Description	JMobile current conformity level (V2.0 SP1)
11.10(a)	(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Customer is responsible for validation of the system. Audit Trail log files are maintained in a proprietary, non-editable format that will prevent manipulations.
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.	Alarm buffers can be saved as readable files. Audit Trail buffers can be saved as readable files.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Alarm buffers and Audit Trail buffers can be saved in a proprietary, non-editable format for backup purposes.
11.10(d)	Limiting system access to authorized individuals.	JMobile uses local user management. Encryption used for passwords. Logout after inactivity period. Check password length and format.
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.	JMobile Audit Trail buffers are not editable.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Customer responsibility. Must be implemented with appropriate JMobile programming.

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.	JMobile Security provides appropriate local user management.
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.	Customer responsibility. Must be implemented with appropriate JMobile programming.
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.	Customer responsibility. EXOR provides training material and services.
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.	Customer is responsible for establishing appropriate procedures.
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. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Customer is responsible for establishing appropriate procedures.
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.	JMobile has been designed for operation in closed systems.
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.	Records contain the following information: (1) User name (2) Date and time (3) Description of action performed
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).	
11.70	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.	
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	JMobile Security functions guarantee that user name is unique within the application. Customer is responsible that a User identification is assigned to only one individual.
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.	Customer responsibility.
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. (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.	Customer responsibility.
11.200(a)	(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	JMobile Security functions are based on the combination user/password. (3) customer is responsible for ensuring appropriate procedures.

	<p>signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.</p> <p>(2) Be used only by their genuine owners; and</p> <p>(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.</p>	
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.	JMobile currently does not support biometrics.
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.	JMobile Security functions guarantee that combination user name and password is unique within the application.
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).	
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.	JMobile Security functions allow users be disabled by administrators. Users can be assigned to a default group without any authorization. Disabled users will be present in the systems in historical logs but will not be allowed to log in. Passwords can be reset by administrators.
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.	
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.	Customer is responsible for ensuring appropriate measures.