

System Assessment Report
Relating to Electronic Records and Electronic Signatures
FDA 21 CFR Part 11 | EudraLex, Volume 4, Annex 11¹

System: IONIC App
(Version 1.0)²

¹ see EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines

² The assessment is made for version 1.0,x where the last number represents the patch version. Since the ERES Assessments result is independent of the patch level, the outcome is valid generally for the entire IONIC App Version 1.0 series

0 General System Information (regarding ERES relevance)

Electronic Records (Section 0)

Is the system used to manage (create, manipulate, administer, restore, transmit or archive) electronic records?

Name the electronic records considered in this assessment?

☒ **Yes³** / ☐ **No**

Basically, the answer to this question depends on the application of IONIC App, and has to be given by the respective GxP process owner.

The following data are maintained by IONIC App and can therefore be used as Electronic Record:

Sample (statistics, calibration curves, curve overlay), Subsample (sub-sample data, variables, curves, measuring points lists, raw data, calculations), Method

Closed System / Open System (Section 2)

Is the computerized system a closed or open system?

☒ **Closed system**

☐ **Open system (Section 2)**

IONIC App can connect to a cloud-based repository service (called Metrohm Data Service⁴) using LAN/WAN connection.

Electronic Signatures (Sections 3 to 7)

Offers IONIC App the ability to sign electronic records by means of electronic signatures?

What type of electronic records can be signed electronically?

☒ **Yes** / ☐ **No**

Electronic record types "Subsample" and "Method"

Assessment prerequisite

This ERES assessment is performed with the precondition that IONIC App is setup⁵ for GxP compliant use:

ERES compliance: ☒ **Activated** / ☐ **Deactivated**

³ For the purpose of this ERES assessment, it is assumed that IONIC App supports GxP processes, including processing of electronic records.

⁴ the "Metrohm Data Service" itself is out of scope of this System Assessment Report

⁵ setting located in "Work area" > "Settings" > "Security"

1 Procedures and Controls for Closed Systems

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
1	11.10 (a) A11: Principle A11:1 A11:2 A11:3 A11:4	Validation, IQ, OQ	Is the system validated?	O		The operator⁷ is solely responsible for the validation of the system. The responsibility of the supplier is to supply a system that is capable of being validated. This is supported by the internal Metrohm quality management system, which can be audited on request. Metrohm runs a certified quality management system based on the requirements of ISO 9001:2015. In this respect, Metrohm offers a range of validation documents and services: Conformity certificates, predefined IQ and OQ documentation, whose execution can be performed at the operator's premises.
2	11.10 (a) A11:6 A11:8.2 A11:9	Audit Trail, Change, Printout, Manual Data Entry, Electronic Record, Operator Entries	Is it possible to discern invalid or altered records?	X		Chapter 0 lists the relevant record types considered as 'Electronic Records' in the IONIC App. Record modification: • Method alteration forces the creation of a new method version. • Subsample modifications (reprocessing, i.e., recalculation and/or reevaluation) generate a new determination version. For better recognition, modified subsamples are marked with a special (pencil) symbol. Existence of the new version is recorded in the audit trail. • Previous determination versions can always be retrieved from the determination history. • Previous method versions can always be retrieved in the system.

⁶ Reference to the 21 CFR Part 11 ('11.nn') and/or EU GMP Guidelines Annex 11 ('A11:...') paragraphs;

The following Annex 11 paragraphs are not referenced since they apply definitely to the operator only: A11:11 "Periodic Evaluation", A11:13 "Incident Management", A11:15 "Batch Release" and A11:16 "Business Continuity"

⁷ In this System Assessment Report the term „Operator“ refers to the individuals acting on behalf of the regulated company; Depending on the context this might be the Process Owner (overall accountable for the operation), or an actual user (e.g. laboratory staff), or a support person (taking care for maintenance etc.)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
						Discern invalid records: • Errors raise an error message, which is displayed to the operator. • Events of the type “Information” or “Warning” that happen during a determination are displayed to the operator, while an error aborts the determination process. • As part of a method conditions for solutions and sensors can be defined to detect the use of inappropriate solutions/sensors. • Invalid calibration values are raising a warning. • Specific invalid data (e.g., operator enters values out of a predetermined range) are automatically recognized by the IONIC App alarmed and the process is paused.

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
3	11.10 (b) A11:8	Report, Printout, Electronic Record	Is the system capable of producing accurate and complete copies of electronic records on paper?	X		IONIC App creates complete reports of the electronic records in PDF format, which can be sent to a printer accessible in the LAN, or stored on a USB drive, or in the Metrohm Data Service for printing elsewhere. The following reports are provided with the system: • for Method data: Parameters • for Sample data: Statistics, Calibration • for Subsample data: Equipment, Results, Chronology Every page of the report is numbered and contains the timestamp of the report generation. Once a signed method is used in a determination the signing status is recorded in the subsample report. The method report includes the method version number. Audit trail data can be printed via export into a CSV⁸ format where the created file is stored on a USB drive from which it can be printed with many commonly available applications. Various types of predefined subsample and/or method reports can be printed as printouts automatically by means of a "REPORT" command in a method during an analysis. Because the "Chronology" report does not contain all change information the audit trail information must be inspected in addition for the complete picture.
4	11.10 (b)	Report, Electronic Record, FDA	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	X		Since IONIC App generates reports in PDF format from the electronic records (see no. 3), these PDF files can be stored on a USB drive, or using the Metrohm Data Service, and made available for inspection, review or copying. The audit trail of a sample and subsamples can be exported as CSV file.
5	11.10 (c) A11:7.1	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	X/O		The operator is solely responsible for record storage/archiving.

⁸ CSV: Comma Separated Values

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
	A11:7.2 A11:17					The system monitors the status of unsaved data (e.g., modified sample profile data) and notifies the user before unsaved data are going to be lost. The system stores all data permanently in its database. The database can be backed up by the operator (together with system settings and device data). The backup file is always encrypted with a system password, and in addition by an operator-set password – if applicable. Based on this backup data the operator is able to restore the database and system settings. Restoring the device configuration data backup is available to service personnel only. In addition to the storage in the IONIC App database, IONIC App is able to export the electronic records (samples, subsamples, methods, audit trail data) on a USB drive: - Method data in IOM format, - Sample/Subsample data in IOS format, - Subsample data in CSV format. IOM and IOS formatted files can be imported afterwards into a IONIC App database. IOM and IOS formatted files can be stored using the Metrohm Data Service too. In addition, all electronic records can be stored in PDF format on paper (via printout), or electronically on a USB drive, or using the Metrohm Data Service. IONIC App provides backward compatibility for its data format, i.e. for previous IONIC App versions.⁹ The operator may also decide to consider PDF reports or printouts as relevant records by using IONIC App's reporting functionality (see no. 3 + 4). The audit trail can be exported as CSV file. It is the operator's responsibility to ensure that the correct subset of audit trail entries is exported and to protect the file against modification.

⁹ the backup contains a software version number indicator; access to data of former IONIC App versions might require processing of internal migration steps up to the current software version

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
6	11.10 (d) A11:12	Login, Access Protection, Authorization, User, Administrator, Record access authorizations	Is the system access limited to authorized individuals? Are creations or modifications of roles and access rights recorded?	X		The IONIC App can be set up to support user management, authentication (user account status) and authorization (system access status). Individual user accounts can be assigned to one or more user groups, at which level the access rights are defined. Three user groups are predefined ("Administrator", "Laboratory Manager", "Routine User"), those user groups cannot be modified. In addition, there is the special role "Field Service Engineer" that requires a special USB dongle to use the role. The operator must ensure that access rights are granted to authorized people only. All changes in the user management are recorded in the audit trail.
7	11.10 (e) A11:9 A11:12.4	Audit Trail, Electronic Record, Operator Entries, Reason for Change/Deletion	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records? Does the audit trail (mandatorily) collect the reason for a record change or deletion?	X/O		Chapter 0 lists the relevant record types considered as 'Electronic Records' in the IONIC App. Modifications of these records introduced by the user are recorded in the audit trail with time stamp (date/time; based on the system time of the IONIC App), User ID, and the value changed. Once a determination is started all relevant data are copied into the subsample data set; As such the subsample data are independent of subsequent changes of the master data (e.g. method data). All data relevant to the result are contained in the subsample record (raw data, measuring points list, result, method, equipment elements used, etc. – if applicable). All operator entries are recorded in an automatically generated audit trail including the old and new values. An electronic record modification (method, sample, subsample) requires the user to provide the reason for the change (out of a predetermined list); In addition, the operator can add a comment (free text). Both entry types are logged in the audit trail. Methods: Once a method modification is saved, a new method version is generated. Previous method versions are always retrievable from the method history (read-only mode) and can be printed. Deletion of a method is recorded in the audit trail. A method cannot be deleted as long as a subsample exists that contains this method. A method modification creates a general audit trail entry¹⁰.

¹⁰ indicating the type of modification (i.e. old/new values for simple parameter changes, OR structural change for changes in the method structure)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
						Sample: Once a sample is modified this is generally recorded in the audit trail; the actual details about what was changed are stored with the audit trail of the respective subsample (i.e. that has been changed with the sample change). Deletion of a sample list is recorded in the audit trail. When deleting a sample list, all samples therein are deleted and all subsamples contained in the sample too. Reason and (optional) comment are logged in the audit trail. Subsamples: All data relevant for the result are linked to the subsample (method, used equipment¹¹, and so on). Subsample modifications (e.g. reprocessing) generate a new determination version. For better identification, modified subsamples are marked with a special (pencil) symbol. Previous determination versions are always retrievable from the determination history. If a subsample is deleted all changes that have been applied to this record are still available in the audit trail. Changes that have no impact on the result do not require the operator to enter a reason (e.g. renaming of a sample). The timestamp is either gathered from a NTP server that is configured in the IONIC App, or system time – which is set manually by the operator. Methods and subsamples that are signed on level 2 cannot be deleted. Since the audit trail covers changes after the initial creation only, full traceability of all values of a deleted electronic record requires that the user creates and keeps a report with the initial(!) values of the respective record. Modifications of security and ERES settings, user administration, and configuration data are recorded in the audit trail too.

¹¹ Sample equipment data are locked against modification once a determination has been started

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
8	11.10 (e)	Electronic Record, Overwriting data, Change	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	X		Modification of a method requires creation of a new version of this method, as such the original method values are still available in the previous version. The method modification itself is recorded in the audit trail too. Modification of a subsample is transparently recorded in the audit trail. Modification of a subsample determination (i.e. the analysis was started = analyzed subsample) creates a new determination version, as such the original determination values are still available in the previous version of the determination. The subsample modification itself is recorded in the audit trail too. Previous values of a modified sample are recorded either with the method that was changed with the sample (see values in the previous version), or with the determination that was changed with the sample (see value recording in the audit trail).
9	11.10 (e) A11:7.1	Audit Trail, Retention Period	Is the audit trail of an electronic record retrievable throughout the retention period of the respective record?	X/O		The audit trail is maintained in the IONIC App database. The user is responsible for retaining a working installation of IONIC App throughout the data retention period. The audit trail can be exported as CSV file. It is the responsibility of the user to ensure the integrity of the exported CSV file.¹² The IONIC App database can be backed up; such a backup contains all electronic record and the belonging audit trail.
10	11.10 (e)	Audit Trail, FDA, Inspection	Is the audit trail available for review and copying by the authorities?	X		Besides the audit trail representation in the IONIC App, the audit trail can be exported to a CSV file. Thus, it is available in electronic form and or can be printed on paper. The operator is responsible for ensuring the integrity of the exported CSV file.

¹² Audit trail export into a CSV file can be used to evaluate the audit trail data or to hand over the audit trail data to third parties (e.g. in case of an inspection)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
11	11.10 (f)	Control over sequence of steps, Plausibility Check, Devices	If the sequence of processing steps or events is important, are these enforced by the system?	X		Each determination is executed according to the sequence of steps defined in the method. The use of input prompts allows enforcing entry of sample data at the appropriate step in the analytical process. Validation and release of appropriate methods is the responsibility of the operator. IONIC App has various features to support this process (e.g., editing of method requires appropriate user group rights). Methods can be signed electronically; if such a method is signed with a signature at level 2 the method is locked against further modifications. Methods signed on level 2 can only be edited if a new version of the method is created beforehand. Users can be limited to use released methods only (signed at level 2) while executing a subsample analysis¹³.
12	11.10 (g) A11:12.1	Login, Access Protection, Authorization, User, Administrator	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	X		Access to the IONIC App (and thus control of instruments) is available for user accounts with system access = "Granted"¹⁴ and user account status = "Approved"¹⁵ only. Access rights that are assigned to a user group control which functions and data are accessible or executable. Once a user joins a user group he/she inherits the access rights of this user group. The person responsible for user administration must ensure that access rights are granted to authorized individuals only. IONIC App provides configurable measures to control password complexity¹⁶ and functions to control authorized access¹⁷. Subsamples and methods can be signed electronically. There are two signature levels. Signature rights are tied to user groups (method and subsample signatures separately). The same individual cannot sign on both, signature level 1 and 2. User rights can be limited so that only signed methods can be used.

¹³ if a method is modified that is signed on level 1 a new method version is created¹⁴ this is called "Authorization" in the IONIC App¹⁵ this is called "Authentication" in the IONIC App¹⁶ e.g. minimum password length, mandatory characters (upper/lower case, numbers, special character), maximum validity period¹⁷ e.g. maximum number of failed login attempts

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control validity of the connected devices? <i>If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g., terminals) does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio-controlled terminals).</i>	X/O		Metrohm instruments: They are recognized as soon as they are connected to the device and are automatically entered in the “Equipment” work area, “Instruments” subsection of the IONIC App. For a determination to be started, all instrument’s functional units required by method must be available. It is also possible to monitor the validity of peripherals, e.g., the calibration of a pH electrode, the titer of a solution. Non-Metrohm instruments (e.g., a balance connected through a serial port): Although a specific port is configured at instrument level, the IONIC App would not recognize (via communication protocol) a modification in the instrument connected to that port. The operator is solely responsible to validate the correct installation of Metrohm and 3rd party instruments.
14	11.10 (i) A11:2	Training, Support, User, Administrator	Is there documented training, including on the job training for system users, developers, and support staff?	X/O		The operator is responsible for training users and supporting staff. Metrohm offers standard training courses for all application fields. Individual training courses can be arranged separately. Metrohm product developers and service personnel receive further training at regular intervals. Training management is part of Metrohm’s ISO 9001:2015 certified quality management.
15	11.10 (j) A11:14a	Policy, Responsibility, Electronic Signature, Signature Impact	Does the electronic signature have the same impact as the handwritten signature? Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	O		If the electronic signature is used, the operator is responsible for raising awareness among users regarding the equivalence of the electronic signature with handwritten signatures (e.g. via training). Control and management of the electronic signature’s impact is in the responsibility of the operator. It must be ensured that each user who is able to sign electronically is aware and trained that the electronic signature has the same impact and consequences as the handwritten signature.
16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	O		The IONIC App has a comprehensive online help that supports users and service personnel. In addition the online help is provided in PDF format too. The operator is responsible for the internal distribution of the system manual (PDF file).

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
17	11.10 (k) A11:4.2 (A11:10)	SOP, Documentation, Manuals, System Documentation, Audit Trail, Logbook	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail (= version history) for creation and modification?	X/O		The system documentation is unambiguously assigned to a dedicated system and software release. Release notes describe the changes compared to the previous software release and are published for each software release. Management of system documentation (filing, distribution, access control) must be ensured by the operator.
18	A11:6	Manual Data Entry, Electronic Record, Operator Entries	Are there checks to verify critical data entered manually?	X/O		The IONIC App can check some manual entries based on predefined rules: • Commands are configured to accept parameters only within a specific range; • For the sample size or other user-defined subsample data requested (at analysis start or during the execution), value limits can be defined by the developer of the respective method. This input verification is limited to a specific configuration and does not necessarily meet the business process needs. Therefore, the operator is responsible for defining the required input controls and ensuring that these are implemented, either by organizational means (e.g., SOPs), or technically (e.g., automatic input verification), typically in the course of the method validation.
19	A11:4.8	Data Migration, Electronic Record	Are electronic data checked for consistency if migrated from one system instance to another (e.g., no change of values or meaning)?	O		Development of the migration functionality of the IONIC App is controlled by the Metrohm's Quality Management System, which is part of the ISO 9001:2015 certification ¹⁸ . In case of an IONIC App upgrade, a database conversion might be necessary ¹⁹ . Then IONIC App converts the old database to the new schema. ²⁰ Nevertheless, data migration needs to be controlled and monitored by an operator-led validation process (see no. 1).

¹⁸ E.g., data migration is regularly verified during regression testing of each IONIC App release.¹⁹ Data migration is done automatically under the hood (without user involvement) with one migration step per upgrade version (i.e. migration from version 2 to version 5 requires the migration steps v2 → v3, v3 → v4, and v4 → v5)²⁰ As a rule IONIC App provides downwards compatibility for older database formats

2 Additional Procedures and Controls for Open Systems

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
20	11.30 A11:5	Data, Encryption, Data Transfer	Is the data integrity of the electronic records protected when they are processed via the Internet? Are data encrypted?	X		IONIC App allows the user to store the electronic records, which are in the application's database, using Metrohm's cloud service (i.e. "Metrohm Data service")²¹. The connection from the IONIC App to the Metrohm Data Service is encrypted (i.e. https). Access to the Metrohm Data Service is controlled by several means: - Each user needs a myMetrohm²² account, - Each user must be member of an Organization Unit, - Each Organization Unit needs a valid subscription, - Each Organization Unit has its own user management, - One user is able to get access to one Organization Unit only, - For each Organization Unit several IONIC Titrators can get registered, - For each IONIC Titrator a registration is necessary, after successful registration an authentication key gets exchanged, - A registration of an IONIC Titrator needs "OAuth 2.0 Device Authorization Grant" of the myMetrohm Login Service, - Device authentication key expires after pre-defined time of device downtime; IONIC App updates authentication key during uptime.
21	11.30 A11:5	Digital Signature	Are digital signatures used to authenticate the involved parties?	X		The use of transport encryption implies the use of digital certificates, which ensures authentication of the communication endpoints involved. In addition, authentication of the involved users is strictly controlled (see no. 6 and 20).

²¹ see no. 5²² account for cloud services managed by Metrohm

3 Signed Electronic Records

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
22	11.50 A11:14c	Electronic Signature	Do signed electronic records contain the following related information: - The printed name of signer, - The date and time of signing, - The meaning of the signing (such as approval, review, responsibility)?	X		All signatures contain the User ID and the username of the signatory, date and time of the signature and its meaning. ²³ This data are stored with each individual signature. On signature level 1 more than one person can sign the record with her/his individual electronic signature. Optionally, a comment can be added to the signature, which is saved together with the electronic signature.
23	11.50	Electronic Signature	Is the above signature information displayed with representations of the signed record (on screen and on paper printouts)?	X		All signature components are displayed on the electronics record and on dedicated printouts thereof: • Signed method: Report "Parameters" • Signed subsample (i.e. determination): Report "Results" and Report "Parameters"
24	11.70 A11:14b	Electronic Signature	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	X		Each signature is securely linked to its respective object. Signature elements cannot be cut, copied, or transferred by ordinary means. A level 1 signature can be withdrawn in case of a modification of the relevant electronic record. Withdrawal of a level 1 signature requires the user to enter a reason. A level 2 signature cannot be revoked. A level 2 signed record can be modified only by creating a new version of the relevant record (which is then unsigned). The signing history of the respective object is recorded in the audit trail.

²³ Electronic signing is available for the following record types: Subsample and method (s. Chapter 0)

4 Electronic Signature (General)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
25	11.100 (a)	Electronic Signature	Are electronic signatures unique to an individual?	X/O		Signatures are executed with the same credentials (User ID and password) that are used for the login operation. The system monitors the unambiguity of the User ID. The operator is responsible for ensuring that multiple individuals do not share the same user account.
26	11.100 (a)	Electronic Signature	Are the credentials for ES ever reused by, or re-assigned to, anyone else?	O		The User ID must be assigned to an individual. The operator is responsible for ensuring that this User ID is not re-assigned to another person. User accounts can be disabled but not deleted (see no. 35).
27	11.100 (a)	Electronic Signature, Representative	Does the system allow the transfer of the authorization for electronic signatures (to representatives)?	O		The operator is responsible for secure and traceable user rights management. The assignment of representatives is part of regular user management. There must be a user management procedure in place..
28	11.100 (b)	Electronic Signature	Is the identity of an individual verified before an electronic signature is assigned?	O		With the initial assignment of signing rights to an individual user account, the identity of the respective person must be verified by the operator (see no. 35).

5 Electronic Signatures (Non-biometric)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
29	11.200 (a) (1)	Electronic Signature	Is the signature made up of at least two identification components, such as an identification code and password, or an ID card and password?	X		Execution of an electronic signature requires entering User ID and password as credentials.
30	11.200 (a) (1)(i)	Electronic Signature	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session).	X		Signing always requires entering both credentials (User ID and password). ²⁴
31	11.200 (a) (1)(ii)	Electronic Signature	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	X		Signing always requires entering both credentials (User ID and password).
32	11.200 (a) (2)	Electronic Signature	Are non-biometric signatures used by their genuine owners only?	O		The operator must ensure that a user uses his/her credentials only.
33	11.200 (a) (3)	Electronic Signature, Falsify Electronic Signature	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	X		Nobody has access to the electronic signature data by ordinary means. Electronic signature data are saved in the IONIC App database. The database itself uses a proprietary format for data storage. Each database is encrypted with a system-specific key. Method or subsample data exported to IOM or IOS files are encrypted and checksum protected, i.e., individuals cannot locate the signature information. Furthermore, modifications would invalidate the electronic record.

²⁴ There is no function like "Signing in a continuous session" in IONIC App

6 Electronic Signatures (biometric)

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
34	11.200 (b)	Electronic Signature, Biometric Electronic Signature	Has it been shown that biometric electronic signatures can be used by their genuine owner only?	N/A		IONIC App does not allow users to sign electronic records using biometric means.

7 Controls for Identification Codes and Passwords

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
35	11.300 (a)	Identification Code, Uniqueness, Password, Identification, Login, Access Protection	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	X		The system ensures that each User ID is used only once within a IONIC App database and therefore each combination of User ID and password can exist only once. Once a User ID has been created it cannot be modified afterwards anymore. It is recommended that the operator organization establish procedures that ensure uniqueness of User IDs organization wide.
36	11.300 (b)	Identification Code, Password, Validity, Identification, Login, Access Protection	Are procedures in place to ensure that the validity of the identification code is periodically checked?	O		The operator is responsible for checking the identification codes periodically. IONIC App supports the operator with a password expiration function (see no. 37).
37	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	X		The validity period of the password can be defined by the administrator role. Once this period has expired, the user must change his/her password.
38	11.300 (b)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	O		The operator is responsible for establishing such a procedure. A user account can be disabled in IONIC App by the administrator role but remains saved in the system without any access rights.
39	11.300 (c)	Identification Code, Loss of ID card, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	O		The operator is responsible for establishing such a procedure. The password of the relevant user account can be reset by the administrator role. Alternatively, the corresponding user account can be deactivated in the IONIC App by the administrator role (but remains in the system without any access rights).
40	11.300 (c)	Loss of / compromised ID card, Electronically disabling ID card	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	N/A		IONIC App does not use hardware tokens or devices for user identification.
41	11.300 (c)	ID card, Replacement	Are there controls over the temporary or permanent replacement of a device?	N/A		IONIC App does not use hardware tokens or devices for user identification.

Run no.	Ref. ⁶	Topic	Question	Yes	No	Comments
42	11.300 (d)	Unauthorized Use, Login, Access Protection	Are there security safeguards in place to prevent and/or detect attempts of unauthorized use of user identification or password?	X/O		After n subsequent incorrect authentication attempts (the number can be defined by the administrator¹⁷) the user account is locked. Also using the wrong User ID ↔ password combination when signing an electronic record will lock the user account as well. Any login attempt (successful or not) is logged in the audit trail. As such, suspicious activities can be detected by means of an audit trail review. The operator is responsible for managing the audit trail review process. IONIC App supports the administrator in implementing security safeguards to prevent and/or detect attempts of unauthorized use of user identification or password (see no. 6).
43	11.300 (d)	Unauthorized Use, Login, Access Protection, Inform management	Is there a procedure in place to inform the responsible management about unauthorized use of user identification or password?	O		The operator is responsible for establishing such a procedure. The audit trail records unsuccessful authentication attempts, which can be checked in an audit trail review (see no. 42).
44	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic testing of tokens and cards?	N/A		IONIC App does not use hardware tokens or devices for user identification.
45	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does the token or card testing verify that there have been no unauthorized alterations?	N/A		IONIC App does not use hardware tokens or devices for user identification.

Legend

- X Applies to system
- O Implementation is in the operator's responsibility
- N/A Not applicable to the system

8 Indices

Reference to the page number:

A

Access Protection.....	7, 10, 18, 19
Access to Documentation.....	11
Administrator	7, 10, 11
Archiving	5
Audit Trail	3, 7, 9, 12
Authorization	7, 10

B

Balance	11
Biometric Electronic Signature	17

C

Change.....	3, 9
Compromised ID card	18
Connection	11

D

Data.....	13
Data Migration.....	12
Data Transfer	13
Devices	10, 11
Digital Signature.....	13
Disable User Access	18
Distribution of Documentation	11
Documentation	11, 12

E

Electronic Record	3, 5, 7, 9, 12
Electronic Signature	11, 14, 15, 16, 17
Electronically disabling ID card	18
Encryption	13

F

Falsify Electronic Signature	16
FDA.....	5, 9

I

ID card	18, 19
Identification.....	18
Identification Code	18
Inform management.....	19
Input data.....	11
Inspection	9
IQ	3

L

Logbook	11, 12
Login	7, 10, 18, 19
Loss of ID card.....	18

M

Manual Data Entry	3, 12
Manuals	11, 12
Modification of ID cards	19

O

Operator Entries.....	3, 7, 12
OQ	3
Overwriting data	9

P

Password	18
Password Expiry	18
Plausibility check.....	10

Policy	11
Printout	3, 5

R

Reason for Change/Deletion	7
Record access authorizations.....	7
Replacement	18
Report.....	5
Representative	15
Responsibility	11
Retention Period.....	5, 9

S

Sequence	10
Sequence of steps	10
Signature Impact	11
SOP	12
Support.....	11
System Documentation.....	11, 12

T

Terminals.....	11
Testing of ID cards	19
Training.....	11

U

Unauthorized Use	19
Uniqueness.....	18
User	7, 10, 11

V

Validation.....	3
Validity	18

Reference to the run number of the entry:**A**

Access Protection	6, 12, 35, 36, 37, 38, 39, 40, 42, 43, 44, 45
Access to Documentation	16
Administrator	6, 12, 14
Archiving	5
Audit Trail	2, 7, 9, 10, 17
Authorization	6, 12

B

Balance	13
Biometric Electronic Signature	34

C

Change	2, 8
Compromised ID card	40
Connection	13
Control over sequence of steps	11

D

Data	20
Data Migration	19
Data Transfer	20
Devices	11, 13
Digital Signature	21
Disable User Access	38, 39
Distribution of Documentation	16
Documentation	16, 17

E

Electronic Record	2, 3, 4, 5, 7, 8, 18, 19
Electronic Signature	15, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34

Electronically disabling ID card	40
Encryption	20

F

Falsify Electronic Signature	33
FDA	4, 10

I

ID card	41, 44, 45
Identification	35, 36, 37, 38, 39
Identification Code	35, 36, 38, 39
Inform management	43
Input data	13
Inspection	10
IQ	1

L

Logbook	16, 17
Login	6, 12, 35, 36, 37, 38, 39, 42, 43
Loss of ID card	39, 40

M

Manual Data Entry	2, 18
Manuals	16, 17
Modification of ID cards	45

O

Operator Entries	2, 7, 18
OQ	1
Overwriting data	8

P

Password	35, 36, 37, 38, 39
Password Expiry	37

Plausibility Check	11
Policy	15
Printout	2, 3

R

Reason for Change/Deletion	7
Record access authorizations	6
Replacement	41
Report	3, 4
Representative	27
Responsibility	15
Retention Period	5, 9

S

Sequence	11
Signature Impact	15
SOP	17
Support	14
System Documentation	16, 17

T

Terminals	13
Testing of ID cards	44
Training	14

U

Unauthorized Use	42, 43, 45
Uniqueness	35
User	6, 12, 14

V

Validation	1
Validity	36, 37, 38, 39