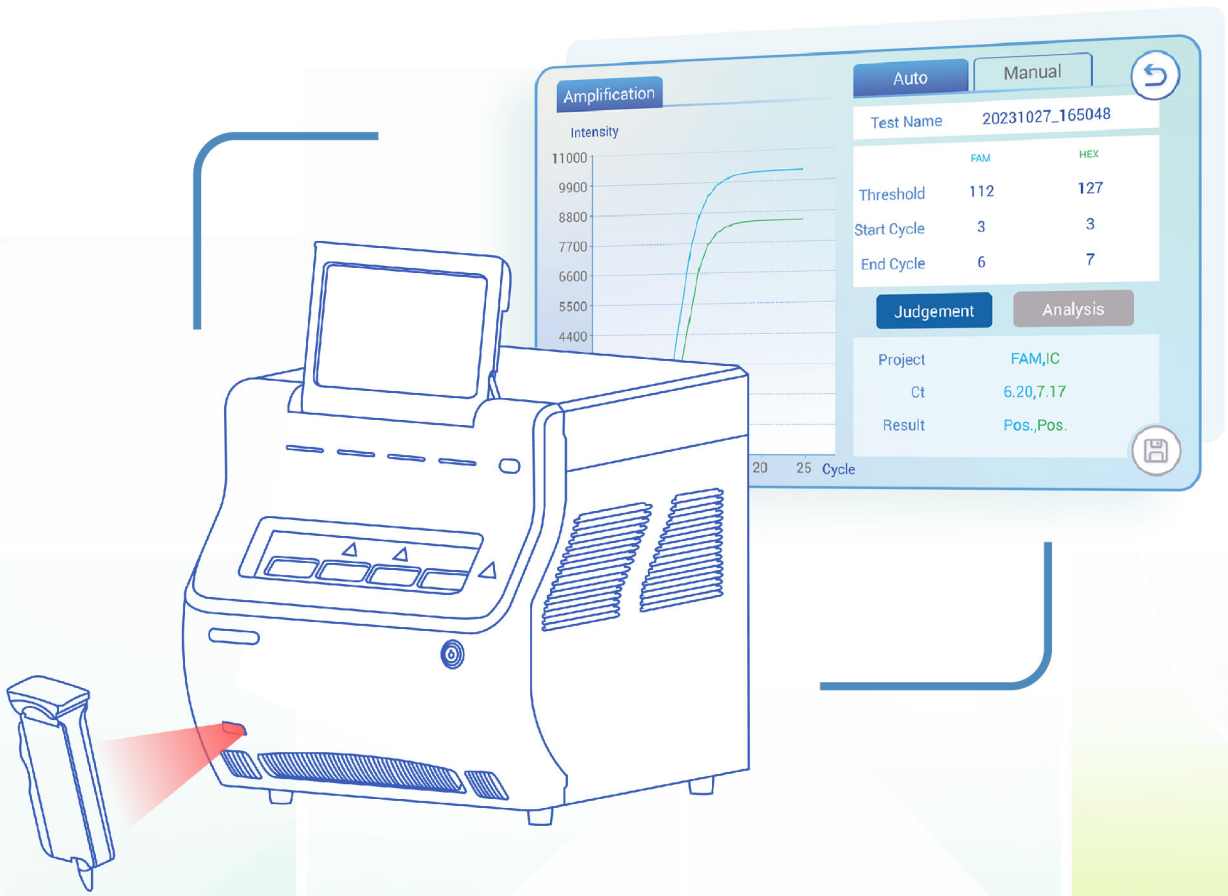
SHENTEK

Support for 21 CFR Part 11 and Annex 11 Compliance:

AdvSHENTEK DetectInnova System



Huzhou Shenke Biotechnology Co., Ltd.

Overview

US FDA Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its EU analog, Eudralex Chapter 4, Annex 11, describe the requirements for electronic records and electronic signatures for regulated pharmaceutical organizations. Released in 1997, 21 CFR Part 11 has been enforced since 1999. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with integrity.

This white paper serves as a valuable resource for users of the AdvSHENTEK DetectInnova System, which shall comply with these regulations. Users and their organizations are responsible for ensuring that the functions provided by the AdvSHENTEK DetectInnova System are used appropriately, thereby ensuring the safe storage of laboratory data and compliance with regulatory requirements.

It is the responsibility of the user and their organization to ensure that the technical controls provided by AdvSHENTEK DetectInnova System are used appropriately to achieve compliance-readiness for laboratory data acquisition and data processing. The user's organization shall establish procedural controls--standard operating procedures (SOPs)—to address relevant nontechnical requirements. Governance, for example as an internal audit program, shall also be established to assure that system operators follow the SOPs.

Appendix 1 provides a detailed description of how AdvSHENTEK DetectInnova System supports users and their organizations in achieving the requirements of each section of 21 CFR Part 11 and the related sections of EU Annex 11. The descriptions assume that the system access, including instrument hardware and software, is controlled by the staff responsible for the electronic records contained on the system. Thus, the system is designed as a "closed system" as defined in 21 CFR Part 11.3(b).

21 CFR Part 11

21 CFR Part 11 covers three specific elements of a regulated laboratory's operation:

- Security of electronic records
- Attribution of work
- Electronic signatures (if used)

Security

Security can be interpreted as "the right people, having the right access, to the right information." Regulated organizations must be able to both verify the identity of system users and limit system access to trained, authorized individuals (11.10(d), (i) and (g); 11.100(b)). Because laboratory staff have different responsibilities based on their job assignments, data access must be segregated and defined such that certain users have certain types of access to certain sets of data while potentially having different access to other data sets.

Attribution of work

Attribution of work refers to documenting the "Who, what, when, where and why?" of work performed. Automated audit trails independently record users actions thus connecting laboratory staff to the work they perform. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

- **Who:** clearly identifies the person responsible for the particular action that creates, modifies, or deletes a record.
- **What:** is the action that took place, including, if applicable, the old value and the new value contained in the record.
- **When:** unambiguously declares the date and time the action took place.
- **Where:** clearly identifies the impacted record.
- **Why:** explains the reason for a change to a regulated record. The reason is often selected from a list of pre-defined reasons to provide consistency and to enable searching and sorting of entries.

E-Signatures

While 21 CFR Part 11 does not require the use of eSignatures, it does provide regulations for their use when they are used. In this case, the system must ensure that eSignatures:

- Are irrevocably linked to their respective records.
- Show the full name of the signer, date and time, as well as the meaning of, or reason for, the signature (such as review, approval, responsibility, or authorship).
- Are present whenever the signed records are displayed or printed.

Appendix 1.

Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations using AdvSHENTEK DetectInnova System

Appendix 1 Table Notes:

Column one

The table addresses 21 CFR Part 11 requirements in the order that they are presented in the US FDA Guidance (View on FDA.gov). Related requirements such as those found in EU Annex 11 are included in each section.

Column two

Column two lists all requirements of 21 CFR Part 11 and Annex 11. “System” refers to the analytical system used to acquire and process data. Most requirements are fulfilled by either technical controls (i.e., software functionality) or procedural controls (i.e., SOPs). Technical controls are controls provided by the software and hence the software supplier, while procedural controls are the responsibility of the user organization.

Column three

Some requirements involve both technical and procedural controls. Responsibilities for each requirement are listed in column three. “S” refers to analytical system supplier. “U” refers to the user organization.

Column four

Column five indicates with a “yes” or “no” whether the requirement can be satisfied using the technical controls provided in AdvSHENTEK DetectInnova System. N/A is not applicable to AdvSHENTEK DetectInnova System.

Column five

Column five explains how the regulatory requirement can be satisfied using the technical controls provided by AdvSHENTEK DetectInnova System. Column five also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 / Annex11	Requirements	S,U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(a)	1.1 Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S,U	Yes	SHENTEK has conducted extensive validation of the performance of the fully automated nucleic acid testing analysis system for extraneous agents by assessing its accuracy, reliability, and consistency. This statement in no way relieves customers of their responsibility to validate their computerized systems for their intended use in accordance with regulatory requirements. User organizations are still required to validate the system in line with regulatory expectations. The system is a closed system that can produce relevant documentation. The system is a closed system that does not allow the addition of input files that could affect system documentation. All operations on data generated by the system within the instrument's operating environment will be recorded, and records created through operations within the instrument can only be newly created and will not overwrite existing records. SHENTEK has fully tested and validated the system to ensure its accuracy, reliability, and consistent intended performance. The system maintains the following regulated records: • Audit Trail • Log Data • Instrument Method Data • Exception Data • Report All operations performed on data generated by the system within the instrument's operating environment will be recorded. Furthermore, any records created through operations within the instrument can only be newly generated; they cannot overwrite existing records.
Annex 11	1.2 Is infrastructure qualified?	U	N/A	Qualification of infrastructure such as servers and networks are the responsibility of the user organization.

2. Accurate copies and secure retention and retrieval of records

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(b)	2.1 Is the system capable of generating accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA?	S	Yes	Records can be printed in paper form or generated as electronic PDF files. These copies are accurate and complete, and their content is consistent with the original records.
Annex 11	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	S	Yes	Records can be printed in paper form or generated as electronic PDF files.

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part11 11.10(c)	2.3 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	S,U	Yes	All raw data, metadata, and result data generated by the system are stored in a secure location within the instrument. The system allows for the backup of reports and the audit trail.
Annex 11	2.4 Are data checked during the archiving period for accessibility, readability and integrity?	U	N/A	The user organization is responsible for ensuring the accessibility, readability, and integrity of the data during the archiving period. The system is designed to ensure that archived data is accessible, readable, and non-modifiable.
Annex 11	2.5 If relevant changes are made to the system (e.g. computer equipment or programs), is then the ability to retrieve the data ensured and tested?	S,U	Yes	The system is designed to read data from historical versions. The user organization is responsible for ensuring the readability of this data during implementation and validation.
Annex 11	2.6 Are data secured by both physical and electronic means against damage?	S,U	Yes	All records of the system are stored in protected locations. It is the user organization's responsibility to prevent physical damage to hardware that generates and retains data. It is also the user organization's responsibility to implement backup and disaster recovery mechanisms.
Annex 11	2.7 Does the system allow performing regular backups of all relevant data?	S,U	Yes	The system has facilities to allow for the administrator to perform periodic backups of the database.
Annex 11	2.8 Is the integrity and accuracy of backup data and the ability to restore the data checked during validation and monitored periodically?	S,U	Yes	It is the responsibility of the user organization to ensure the integrity and accuracy of the backed up data, and also to check, validate and monitor restored data periodically.

3. Authorized access to systems, functions, and data

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(d)	3.1 Is system access limited to authorized persons?	S,U	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. The system does not allow the creation of identical user IDs.
	3.2 Is each user clearly identified, e.g., though his/her own user ID and Password?	S,U	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. It is the user organization's responsibility to ensure that each authorized person has a unique user identity.

4. Electronic audit trail

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(e)	4.1 Is there a secure, computer-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records?	S	Yes	The system maintains the following audit trail records: • Exception Data • Setting-Related Modifications • User Management • Login • Logout • Run Experiment • Save Experiment • Export Experiment • Import Experiment All operations performed on files stored in the system are recorded in a secure, system-generated, timestamped activity log, which also documents the reasons for the changes. This log can be backed up, exported, and printed. Audit trail records cannot overwrite existing records and can be sorted and searched.
FDA GLP*	4.2 Does the audit trail record who has made which changes, when and why?	S	Yes	The activity log within the system lists the dates and times of modifications and changes, along with the user IDs.
Annex 11	4.3 Can the system generate printouts indicating if any of the e-records has been changed since the original entry?	S	Yes	The primary application is responsible for tracking changes in the audit trail of electronic records. Electronic records are stored within the system, which logs subsequent updates to the file in the activity log, allowing end-users to export and print them.
FDA GMP**	4.4 Does the audit trail include any modifications of an established method employed in testing? 4.5 Do such records include the reason for the modification?	S	Yes	The device records all records and does not accept access control. All internal changes record the reasons.
	4.6 Is the audit trail function configured to be always on and can it not be switched off by system users?	S,U	Yes	Audit trails are always on and cannot be deactivated by any user.
Annex 11	4.7 Is audit trail available to a generally intelligible form for regular review?	S	Yes	The activity log within the system is designed to be easy to review, allowing end-users to export and print it.
	4.8 Can audit trail contents be configured such that only relevant activities are recorded for realistic and meaningful review of audit trail information?	S	Yes	The system supports filtering the activity log before displaying the content to meet the preferences of users reviewing the information.
Part 11 11.10(e)	4.9 Is previously recorded information left unchanged when records are changed?	S	Yes	The system records all data input additions, changes, and deletions. If a file stored in the system is changed, it will be saved as a new revision of the original, and the original remains unchanged.

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(e)	4.10 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?	S	Yes	The audit trail information of the system is stored in electronic records. The activity log information stored in the system files is associated with electronic records and cannot be separated from them.
Part 11 11.10(e)	4.11 Is audit trail available for review and copying by the FDA?	S,U	Yes	The audit trails can be reviewed and printed.
Annex 11	4.12 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?) ?	S	Yes	The system is capable of generating corresponding documentation and exporting it for the creation of printed versions.

* OECD Series On Principles of Good Laboratory Practice and Compliance Monitoring Number 17:
Advisory Document of the Working Party on Good Laboratory Practice, Application of GLP Principles to Computerised Systems, 9 November 2022
** Data Integrity and Compliance with Drug CGMP, Questions and Answers, December 2018

5. Operational and device checks

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(f)	5.1 Are there operational system checks to enforce permitted sequencing of steps and events, as appropriate?	S	N/A	The user organization is responsible for specifying and implementing procedural controls.
Part 11 11.10(g)	5.2 Are there 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?	S	Yes	The system supports the configuration of different user roles to control access to content and specific operations. It performs authority checks to ensure that only authorized individuals can: • Use the system, • Electronically sign records, • Access operational or computer system input/ output devices, • Alter records, or • Perform operations.
	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S	Yes	The identity of operators taking action in the system is recorded in the both the audit trail and activity log.
Part 11 11.10(h)	5.4 Does the system allow to use device checks to determine, as appropriate, the validity of the source of data input or operational instruction?	S	N/A	If a fault occurs during instrument operation, it will be recorded in the Exception log and the instrument's alarm indicator will turn red. • QR-coded Reagent Cartridge: A cartridge bearing a unique QR code containing batch information and other relevant data. • Method Code: A code corresponding one-to-one with the methods contained within the cartridge. These codes are pre-stored in the instrument. • Report: The report content comprises all necessary elements, including the method used, reagent cartridge identifier, operator ID, and timestamps.

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(i)	5.5 Is there documented evidence that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	S,U	Yes	It is the responsibility of the user organization to maintain documented evidence that the persons who develop, maintain, or use electronic record and electronic signature systems have the education, training, and experience needed to perform these tasks. All software professionals involved in development this system have received training in relevant aspects of data integrity.
Part 11 11.10(j)	5.6 Is there a written policy that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification?	U	N/A	It is the responsibility of the user organization to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
	5.7 Have employees been trained on this procedure?	U	N/A	It is the responsibility of the user organization to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
Part 11 11.10(k)	5.8 Are there appropriate controls over systems documentation including:(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	U	N/A	It is the responsibility of the user organization to establish systems documentation.
Part 11 11.10(i)	5.9 Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation?	S,U	Yes	It is the user organization responsibility to document the validation and configuration efforts through version control documents (specification, protocol, traceability matrix, summary reports, etc.) SHENTEK follows the lifecycle with defined documentation, programming and testing guidelines. The documentation can be reviewed as required.

6. Data integrity, date, and time accuracy

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Annex 11	6.1 Are computerized systems exchanging data electronically with other systems including appropriate built-in checks for the correct and secure entry and processing of data?	S	N/A	In this case, the system does not exchange data with other systems; it merely stores data generated and processed by other systems. The system ensures the secure and reliable transfer of files.
Annex 11	6.2 Is there an additional check on the accuracy of the data?	S,U	N/A	The user organization is responsible for defining additional validation procedures and ensuring the accuracy of the data.

7. Control for open systems (only applicable for open systems)

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Annex 11	7.1Are computerized systems exchanging data electronically with other systems including appropriate built-in checks for the correct and secure entry and processing of data?	S	N/A	In this case, the system does not exchange data with other systems; it merely stores data generated and processed by other systems. The system ensures the secure and reliable transfer of files.
Annex 11	7.2 Is there an additional check on the accuracy of the data?	S,U	N/A	The user organization is responsible for defining additional validation procedures and ensuring the accuracy of the data.

8. Electronic signatures – signature manifestation and signature/record linking

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part11 11.50(a)	8.2Do signed electronic records 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? 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	S	N/A	The signed electronic records must include signature-related information that clearly indicates all of the following: 1. The signer's unique system identifier; 2. The date and time of signatureapplication (including time zone); 3. The significance (e.g., review, approval, authorization) associated with the signature.
Part11 11.50(b)	8.3 Are the items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section subject to the same controls as for electronic records and are they included as part of any human readable form of the electronic record (such as electronic display or printout)?	S	Yes	Electronic records can be clearly displayed on the instrument's built-in display, exported as PDF files, and printed for physical archiving. These records contain information associated with all of the following: 1. The signer's unique system identifier; 2. The date and time of signature application (including time zone); 3. The significance (e.g., review, approval, authorization) associated with the signature.
Part11 11.70	8.4 Are electronic signatures and handwritten signatures 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?	S	Yes	Electronic signatures are an integral part of their associated electronic records, and the system prevents their modification, overwriting, or deletion. Physical handwritten signatures are not processed by the system; this requirement shall be governed by the user organization through procedural controls.

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part11 General provisions	8.5 Is there a user specific automatic inactivity disconnect measure that would "de-log" the user if no entries or actions were taken within a fixed short time frame?	S	Yes	The automatic session lock allows the user organization to set a period of time after which the user will be automatically logged out.
Annex 11	8.1 When electronic signatures are used, do they have the same impact as hand-written signatures within the boundaries of the company? Are they permanently linked to their respective record? Do they include the time and date that they were applied?	S,U	Yes	The user organization shall establish the legal impact of electronic signatures. Signatures are permanently linked to their respective records. Electronic signatures use a combination of user passwords. When logging into the system, the electronic signature is associated with the username, and all subsequent operations are labeled with the username.

9. Electronic signatures general requirements and signature components and controls

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	S,U	Yes	The system implements electronic signatures through two mandatory elements: a unique user ID and password. Duplicate user IDs are prohibited. Each user possesses a distinct login identity and an associated electronic signature that cannot be reused by others.
Part 11 11.100(b)	9.2 Does the organization verify the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	U	N/A	It is the responsibility of the user organization to verify the identify of staff before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature.
Part11 11.100(c)	9.3 Are persons using electronic signatures, prior to or at the time of such use, certified 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?	U	N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.
	9.4 Do persons using electronic signatures, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	U	N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part11 11.200(a)(1)	9.5 Do electronic signatures that are not based upon biometrics employ at least two distinct identification components such as an identification code and password?	S,U	N/A	The system uses login controls. Users are responsible for identification and authentication.
Part11 11.200(a)(1)(i)	9.6 When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components?	S	Yes	Every time an electronic signature is applied, all mandatory signature components must be entered.
	9.7 When an individual executes a series of signings during a single, continuous period of controlled system access, are subsequent signings executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?	S	Yes	Every time an electronic signature is applied, all mandatory signature components must be entered.
Part11 11.200(a)(1)(ii)	9.8 When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	S	Yes	Every time an electronic signature is applied, all mandatory signature components must be entered.
Part11 11.200(a)(2)	9.9 Are controls in place to ensure that electronic signatures that are not based upon biometrics are used only by their genuine owners?	S	N/A	The user organization is responsible for ensuring that usernames and passwords are known only to the assigned individuals and are traceable to each user.
Part11 11.200(a)(3)	9.10 Are the electronic signatures 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?	S,U	Yes	Any user other than the owner who wishes to use the electronic signature requires the voluntary cooperation of the user and the system administrator.
Part11 11.200(b)	9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	S	N/A	The system does not support biometric authentication.

10. Controls for identification codes and passwords

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part11 11.300(a)	10.1 Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	S,U	Yes	The system does not allow duplicate user IDs. Each user has a unique login name and a unique signature that cannot be used by other users.
Part11 11.300(b)	10.2 Are controls in place to ensure that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	S,U	Yes	Password expiration policies are configurable locally within the application. The user organization shall configure password expiration intervals based on a documented risk assessment, which may include requiring password resets upon login.
Part11 11.300(c)	10.3 Are there procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromise 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?	U	N/A	The system supports authentication solely via user ID and password; it does not accept alternative methods such as security tokens or smart cards.
Part11 11.300(d)	10.4 Are there transaction safeguards in place 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?	U	N/A	It is the responsibility of the user organization to establish these procedures. Identity verification methods such as tokens or cards are not supported.
Part11 11.300(e)	10.5 Are there controls for 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?	U	N/A	The system supports authentication solely via user ID and password; it does not accept alternative methods such as security tokens or smart cards.

11. System Development and Support

Part 11 / Annex11	Requirements	S, U	Yes/No	If Yes, How, Specifically, is the Requirement Satisfied? or If No, What is the Recommendation?
Part 11 11.10(i)	11.2 Is personnel developing and supporting software trained?	S,U	Yes	All appropriate SHENTEK staff are required to be trained. Work instructions are documented in ISO 13485 Scaffold.
Annex 11	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	S,U	Yes	The system is developed within the SHENTEK quality management system, which is defined according to the ISO 13485 standard.

SHENTEK

Huzhou Shenke Biotechnology Co., Ltd.

No. 1366 Hongfeng Road,
Huzhou 313000, Zhejiang Province, China

Mail: info@shentekbio.com
Web: www.shentekbio.com