iBright SAE Software Solution for 21 CFR Part 11 Support

The FDA released the Electronic Records and Signatures Rule, known as 21 CFR Part 11, in August 1997. This rule defines the requirements for use of electronic documents in place of paper documents. Requirements include the system elements, controls, and procedures that are necessary to ensure the reliability of electronically stored records.

21 CFR Part 11 compliance is composed of both procedural and technical requirements. Procedural requirements are the standard operating procedures instituted by the end user, and technical requirements are the functional characteristics of the compliance management software used.

The Invitrogen™ iBright™ SAE Software Solution for 21 CFR Part 11 Support includes the following components that need to be to be installed, activated, and communicating with each other:

- **SAE Administrator Console Software:** used with the iBright Imager and Analysis Software Application Profile to configure the security, audit, and e-signature (SAE) settings for the Invitrogen™ iBright™ instrument and iBright™ Analysis Software—Secure desktop software
- **iBright SAE License:** used to activate the SAE settings for the iBright instrument and iBright Analysis Software—Secure
- **iBright instrument in SAE mode:** firmware mode that connects the iBright instrument to the SAE Administrator Console Software
- **iBright Analysis Software—Secure:** desktop software that connects with SAE Administrator Console Software

The combination of the functional characteristics of iBright SAE software does not alone guarantee 21 CFR Part 11 compliance. Compliance is the consequence of the end user's work process and systems used.

The following details describe how the components of iBright SAE software work together to provide a technical basis for establishing 21 CFR Part 11 compliance support for data acquisition, collection, and analysis steps within the workflow.

Section	Descriptor [1]	Summary	Features
11.10	**Controls for closed systems**		
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System validation	iBright instruments are validated through manufacturing and quality control prior to product release. Additional IQ/OQ services are available upon request. The iBright instrument and iBright Analysis Software—Secure utilizes a proprietary file format that is secure and locked from external tampering. Data integrity is secured through confirmation of an internal checksum. Any audit gaps are reported and documented.
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.	Record generation for inspection	iBright SAE software stores raw data, analysis parameters, results, audit trail for analysis objects, and electronic signature history together in one single proprietary file to allow accurate and complete copies to be regenerated if necessary. Audit trail records for user actions can be viewed via the SAE Administrator Console and exported to a human-readable PDF file that can be printed.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	iBright SAE software manages the raw data, analysis parameters, and results using a database where record accuracy is ensured by calculating an internal checksum of all data files that is verified upon opening the data files in the system (imager or analysis software). Deletion of files can be controlled through user roles and privileges.
11.10(d)	Limiting system access to authorized individuals.	System access limitation	iBright SAE software requires a user to log into the system using a username and password. The system administrator can define roles that can be assigned to each user to restrict access and workflows based on the assigned permissions.
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.	Audit trails	iBright SAE software generates audit records for operations performed by users, including login, logout, image acquisition, image adjustments, image analysis, e-signatures, export and import of data, and changes to the system settings. These records are maintained on the SAE Administrator Console. Audit records include the username, first and last name of the user, date and time of the record, and the machine ID where the record was generated. Audit records cannot be modified. All versions of data files are maintained together and can be viewed and compared.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational checks	iBright SAE software restricts what users can do based on their role and access privileges. A user must log into the software using a username and password, where access to features is based on their assigned role. Actions can be configured to require signatures to control workflows, ensuring data are reviewed prior to completing configured actions.
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.	Authority checks	iBright SAE software ensures that only users that have the proper authority can carry out particular functions based on their roles and access privileges. The software allows user role creation with differing levels of permissions.

Section	Descriptor [1]	Summary	Features
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.	Data and operation validity checks	Methods: iBright instrumentation and software do not contain default methods or method creation. If specific protocols or instrument settings are required, local SOP control should be used. Data input: iBright instruments and software analyze only raw images that cannot be altered. The user sets the areas to be analyzed but cannot alter the values generated for those areas.
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.	Training and user accountability	Thermo Fisher Scientific trains users to operate and maintain the iBright instrument when using the iBright SAE software if requested. Thermo Fisher will train users on the SAE Administrator Console and its use; however, it is the client's responsibility to train employees and assign appropriate roles to a user in order to control access to the system features based on the user's training.
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.	User accountability	iBright SAE software requires use of unique usernames. Access to user data requires the owner of the data to log in using their username and password to prevent modification from another user. Modification of data is not allowed once e-signatures are initiated. Any changes after the e-signatures are recorded creates a new version to which the signatures do not apply. If modification to the data record external to the application is detected, the user is notified, and the file tampering is captured as an audit action record.
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, and (2) revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	System documentation control	iBright SAE software controls revision history for system operation documents and follows the change control procedures when development and modification of system documents are required.
11.30	**Controls for open systems**		**Not applicable. The iBright instrument in SAE mode and iBright Analysis Software—Secure operates as a closed system.**
11.50	**Signature manifestations**		
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all 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.	Signature manifestations	iBright SAE software generates electronic record signatures for an image record that contains the full name of user (as defined in the SAE Administrator Console), username, host ID, date and time stamp plus locale information, and signature meaning.
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).	Signature manifestations	The electronic records generated by the SAE Administrator Console are time, date, and author stamped. Any modifications to the user profile or password are audited. User account ID cannot be changed or deleted. Accounts can only be inactivated.

Section	Descriptor [1]	Summary	Features
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.	Signature/record linking	Electronic signatures are tied to the data record and calculated checksum of the g2i file audit state at the time the signature was generated. Modifications to the file after electronic signing will obsolete any existing signatures, requiring new signatures to be applied. Reports always contain signature information, version information, and page numbers in the header/footer of each page.
11.100	**Electronic signatures**		
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	General electronic signature requirements	iBright SAE software requires user authentication using a unique name and password when applying an electronic signature. All usernames are unique and cannot be reused even if a user has been marked as inactive in the system.
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.	Verification of identity	The organization is responsible for verifying the identity of an individual. The organization is responsible for managing which users and which user roles are authorized to create and edit user accounts.
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.	General electronic signature requirements (certification)	The organization is responsible for management and certification of the electronic signatures.
11.200	**Electronic signature components and controls**		
11.200(a)	Electronic signatures shall employ 2 distinct IDs (ID and password) after first signing; subsequent signings only require a single ID during a continuous session.	Controls for electronic signatures	iBright SAE software and console require both a unique username and password for all signature events.
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.	Controls for electronic signatures	Not applicable.
11.300	**Controls for identification codes/ passwords**		
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.	Uniqueness of ID code and password combination	All usernames must be unique and cannot be reused even if a user has been marked as inactive in the system. The SAE Administrator Console prevents creation of duplicate usernames.
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).	Password aging	An administrator can set up password expiration policies and password criteria. The system can be configured to automatically suspend a user after a specified number of invalid login attempts.
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.	Lost ID and password management	An administrator can reset passwords, configure account lockout policies, and manage user account status (active, inactive, or suspended). A user can reset their password. All changes are recorded in audit history.

invitrogen

Section	Descriptor [1]	Summary	Features
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.	Controls to prevent unauthorized credential use	iBright SAE software can be configured to automatically lock a user account after a specified number of login attempts and can also be configured to lock the screen after a period of inactivity to prevent unauthorized use. SAE Administrator Console can be configured to notify the administrator of events such as entry of incorrect password, suspension of user account, user session timeout, and role deletion.
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.	Periodic testing of ID and password information	An administrator can set up password expiration policies and password criteria. The organization is responsible for establishing periodic testing of ID and password information as required.

Reference

[1] For more information on 21 CFR part 11 and the Electronic Code of Federal Regulations (eCFR) visit fda.gov and ecfr.gov

Find out more about our 21 CFR Part 11 compliance support package at **thermofisher.com/ibrightCFR**

ThermoFisher
SCIENTIFIC