



CERF - 21 CFR PART 11 COMPLIANCE

Subpart B - Electronic Records

Sec. 11.10 Controls for closed systems

11.10	Employ controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	CERF is Compliant	Rescentris CERF provides security controls, audit trails and an e-signature system to ensure the authenticity, integrity and confidentiality of records. The CERF system only accepts records and document updates from authorized users who supply suitable credentials in authenticated sessions. CERF security administration ensures only authorized users can access, update, create or add document information, assuring the authenticity of a document. Record integrity is achieved by providing a complete audit trail and version history, including a copy of the previous and updated record, which can only be accessed by authorized users. CERF offers robust role-based access controls, ensuring highly granular permissions that can restrict unauthorized users from viewing or accessing documents, providing complete confidentiality of records. The CERF user authentication controls, digital signature passwords and signature workflows, and the matching audit trail collectively ensure that the signer can not readily repudiate the signing or the signed electronic record.
	11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	CERF is Compliant	CERF is an electronic lab notebook system for managing lab records and research content. We validate our system to ensure that it performs reliably and consistently for its intended uses, and that that the content and records in the system are maintained accurately and reproducibly. Actions that create, modify, or delete records are recorded in a secure, computer-generated audit trail. Hash codes and digital signatures are stored in the database and used to discern invalid or altered records. Only valid records can be entered into the system. Thorough and systematic testing to validate the performance of CERF is conducted with every release cycle and with each customer installation.
	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.	CERF is Compliant	CERF was designed specifically to enable research organizations to manage scientific content and records in electronic forms that support both reuse of the original formats (data/document objects) and human readable and printable formats suitable for recordkeeping, including inspection, review, and copying by the FDA and other agencies. CERF accomplishes the generation of accurate and complete copies in two ways. The original electronic records are readable, reviewable, and capable of being copied directly within the operating CERF software system by anyway with suitable credentials. For system-independent and software-independent use, CERF creates PDF reports of the contents of the electronic notebooks and pages. These PDF records are stored in the system and are readily retrieved, printed, or transferred to other storage systems. PDF is intended to offer a long-term solution for maintaining copies of records in human readable and electronic form suitable for inspection, review and copying. Individual electronic records can also be copied to desktop applications for these purposes. CERF also supports exports of complete notebooks (with full contents, records, and metadata) in open standard XML format.
	11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	CERF is Compliant	Records are protected by restricting access to authorized users and preventing any unauthorized changes. Users cannot directly modify or delete records in CERF – all actions are mediated by the CERF Server, a secure middle tier which prevents direct access to data. CERF offers a complete document/record control system with system locks when records are checked out for editing, maintenance of all versions of lab records, and the capability to finalize lab records to restrict any further changes. Accurate records are accessible and retrievable throughout their lifecycle in CERF.

11.10(d) Limiting system access to authorized individuals.	CERF is Compliant	<p>The CERF administration program provides an exceptional level of system security. All users must be registered in the system by qualified system administrators, and users are given unique user names and user-designated passwords (that must be changed by the user when assigned or reset by the administrator). CERF has strong name/password controls, and passwords are transmitted only in encrypted form and not stored on the server (only a digital hash code). Users are placed into defined workgroups and have specific, fine-grained role-based access privileges within these workgroups. All records and content in CERF are assigned to workgroups (at the object level as specified directly or as inherited from parent nodes, as set by those given managerial control of workgroups). Users may be in multiple workgroups such that they have different privileges in different projects/notebooks and even different limits on access to templates, actions, and services as well as to the content. Users without minimal (read only) access cannot even view records, while a minimal level of 'Annotator' is required to add notes and links to records, 'Editor' is needed to be able to check out and edit documents, and 'Notebook Editor' role is needed to be able to create or modify the contents of CERF lab notebooks.</p> <p>When users successfully log on to CERF, unique session IDs are created and transmitted with every system communication to prevent inappropriate access. Simultaneous sessions (from multiple workstations) are not permitted for a user, and connecting from a different computer or IP address will close the previous session.</p>
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.	CERF is Compliant	<p>The CERF system includes a complete audit trail function that captures all actions that create, modify or delete data. Audit trails are secure, computer-generated and time-stamped. Recorded fields include creation date and time, update date and time, user name, object modified (by name and system resource object type), action taken, reason (where appropriate), and the new content and metadata. A complete copy of the previous record and its metadata is retained in the system if the content has been placed under version control. The audit trail can be viewed in the CERF web client by authorized CERF administrators, and the database can be queried to generate custom audit trail reports. The audit trail is independent of the database entries for each record, and can be compared to verify that user actions and lab records have been documented correctly.</p>
11.10(e) Record changes shall not obscure previously recorded information.	CERF is Compliant	<p>Documents, data, and notebook entries must be checked out before any changes can be made. Records are locked when contents are checked out. On checking in, the file is stored as a new version, with previous versions stored in the CERF system. The previous version of the metadata is also retained with its record. The version history may be inspected and previous record versions viewed by authorized users.</p>

	11.10(e) 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.	CERF is Compliant	CERF audit trail records are maintained in the database and can be viewed or extracted from the system directly or through queries for the functional life of the software system. The audit trail information cannot be deleted or modified for records in the CERF system. The audit trail documentation is available for agency review, and reports can be made for inspection or copying.
	11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	CERF is Compliant	All actions that create, modify, or delete records occur inside CERF. All actions are operational sequences performed by users authorized to carry out the function and system workflows which verify the events, data management workflows, and the validity of the data and records. CERF actions are defined and limited by the CERF system components and business policies, and are distributed to individuals automatically and securely by the system according to the type of system object, the user's role-based access privileges, and the services available for the selected object. The workflows and actions in CERF are defined by ontologies which cannot be changed by end-users. CERF utilizes internal controls at every step of processes that create or manipulate records to ensure that only appropriate actions and steps of action sequences and workflows are permitted. Such controls include adding new content and annotations to collections (such as Projects and Notebooks), signature workflows, editing and checking in lab records, and validating fields for metadata entry.
	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.	CERF is Compliant	CERF contains security checks to ensure that only authorized and assigned individuals can view, access, create, and modify records. The system requires that an operator has an active CERF account and has logged in with a valid user name and password before any actions can be taken. Once logged in (and until manual or system initiated logout or timeout), a session identifier is passed with every user action to ensure that the operation is specified by the authenticated user. System checks restrict a user from carrying out any action that not authorized for a specific user within a specific workgroup on a specific object/record of a specific type and state (for example, version controlled or finalized). Allowable CERF actions are offered to the operator as dynamically created, context-dependent menus and tool bars. Inappropriate actions cannot be specified (such inputs are not made available in the interface) and would be rejected by the CERF server if somehow delivered (such as if record status changed immediately after selection of an action). Workflows such as digital signatures require that an authorized user with an active CERF session selects a record that the user has contributed to CERF, with requirements that the record is in a signable state, and that the record is owned by a workgroup for which the signer has required co-signers available (if needed) and that the user enters a valid signature password. CERF provides authority checks throughout user operation of the software, including all actions that add or modify records or signatures. If available actions or user access rights change during CERF operation, the effects will be propagated to the user and thereby modify or deny access or other privileges and actions.
	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.	CERF is Compliant	CERF can be configured to accept data or other instructions from specific devices. CERF utilizes the same controls as for user operation, such as requiring a device name and password to create an active session, and may add additional checks, such as validation of data or device IP address requirements. The user organization is responsible for ensuring the security of access to external devices and computers when not operated manually by an authorized CERF user.
	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. 11.10(k) Use of appropriate controls over systems documentation including: 11.10(k)(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 11.10(k)(2) (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Not Applicable	The ability of CERF to meet these requirements is dependent upon the operational controls and procedures established at the client site. Rescentris will assist the user organization in developing and implementing appropriate recordkeeping and electronic signature policies. See further notes below on these topics.

	<p>(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.</p> <p>(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.</p> <p>(k) Use of appropriate controls over systems documentation including:</p> <p>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</p> <p>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>		<p>Rescentris offers training in operation of the CERF software and can make recommendations on recordkeeping and electronic signature practices. The client organization is responsible for ensuring that users have appropriate training and experience to perform their assigned tasks, including maintaining lab records and signing their lab notebooks.</p> <p>The client organization is responsible for developing and following written policies (SOPs) for electronic signatures, CERF signature workflows and lab recordkeeping practices.</p> <p>Rescentris provides standard CERF system documentation, including documents for system administration, user operation, release notes, as well as versioned documentation on system modifications from one software release to the next.</p> <p>Rescentris provides system administration documentation to the client. The client is responsible for disseminating or controlling access to operational and maintenance documents, and also for managing system passwords for administrators.</p> <p>Rescentris supplies new system operation and administration documents and release notes with its installation and updates of CERF. The client organization is responsible for maintaining records and audit trails for any CERF system, CERF component, or policy changes that are made to its system.</p>
11.30	<p>Controls for open systems</p> <p>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.</p>	Not Applicable	CERF is considered a closed system. However, CERF does support all the necessary procedures and controls for managing electronic records in an open system, including encryption of documents and all communications between client and server.
11.50	Signature manifestations		
	<p>11.50(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p> <p>(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.</p>	CERF is Compliant	Signed electronic records in CERF contain the full printed name of signer, date/time when the signature was executed, the meaning of the signature, the role of the signer, and any comments provided by the signer. The system administrator can configure various signature roles, such as Submitter, Peer Reviewer (Witness), Manager/Approve, and Legal/Regulatory acceptance. The CERF administrator can also configure various signature workflows (for example, a single witness for Project documents, a Manager approval for lab SOPs, and two witnesses and a Manager for lab notebook pages). User authority for signatures can be restricted to specific roles, documents/records and work events.
	<p>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)</p>	CERF is Compliant	Electronic signature records are fully secure from unauthorized access, and can be displayed or printed for any electronic record. Notebook printing can be configured to meet the signature requirements of the client.
11.70	<p>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</p>	CERF is Compliant	Once an E-signature (a PKI digital signature in CERF) is applied to a lab notebook page/entry, file object, or other CERF resource, an irrevocable link is established between the signature and the object. The E-signature cannot be deleted, copied or otherwise transferred to falsify the electronic record. A Rescentris PKI digital signature is cryptographically based on the object contents and cannot be falsified or tampered with, nor can the object signed be modified without invalidating the E-signature.

Subpart C- Electronic Signatures

11.100	General requirements		
	11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	CERF is Compliant	CERF enforces the uniqueness of each user ID/password combination, and further requires an additional Digital Signature password. The signature cannot be reused or reassigned to anyone else, even after the original user id has been deactivated or is no longer active. The private key used to generate the digital signature is unique and not known or accessible to anyone else.
	<p>11.100(b) 11.110(c)</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p>	Not Applicable	These are dependent upon the operational controls and procedures established at the client. It is the client organization's responsibility to verify the identity of its CERF users and to maintain and submit records for each user certifying that their electronic signatures (E-signatures, digital signatures) in CERF are intended to be the legally binding equivalent of traditional handwritten signatures. Any additional requirements, certifications, or testimonies regarding an organization's use of electronic signatures is the responsibility of the client. Rescentris can assist its clients in planning and implementing E-signature policies and practices.
11.200	Electronic signature components and controls		
	11.200(a)(1) Electronic signatures that are not based upon biometrics shall: Employ at least two distinct identification components such as an identification code and password.	CERF is Compliant	CERF employs a model that requires a unique user id and password combination for general CERF system access (for the thick client software or the web interface). Users must be logged into CERF using this pair of credentials and have an authorized active CERF session in order to be able to electronically sign a document or record. Then, a third identification component, a digital signature password, is required to complete the signing process.
	11.200(a)(1)(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.	CERF is Compliant	To execute a series of signings, a CERF user must first create an authorized user session by supplying a unique combination of user id and password. During a single, continuous period of controlled system access, the user may then sign numerous or multiple documents, resources, or other lab records by using the third electronic signature component, known only to the signer, which is the digital signature password.
	11.200(a)(1)(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	CERF is Compliant	Each time an individual executes signings not performed during a single, continuous period of controlled system access, the user must first be authenticated by the CERF server with the two signature components of unique user id and password. Then, once authorized, the user may execute one or more electronic signatures with the third signature component, the digital signature password. Any break in the controlled system access – whether manual or automatic – terminates the user session and requires all signature components in order to execute additional electronic signatures.

	<p>11.200(a) Electronic signatures shall:</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>	CERF is Compliant	<p>Executing an electronic signature in CERF requires a unique combination of user id and password plus a third component, the digital signature password. When a system administrator adds a new user or resets a password, the CERF user must change the password before being able to create a new user session. The login password is therefore known only to the individual user, and not to the administrator or to other users. The individual is also responsible for creating or updating the digital signature password, which is encrypted and not known to the administrator or other users. Furthermore, it is actually the private digital signature key that is used to sign lab records, and this key is not known to anyone (it is calculated from the user credentials). CERF electronic signatures are administered and executed to ensure that the only way anyone other than the genuine owner of the could sign with the individual's electronic signature is for a system administrator to collaborate with another user and to supply that other user with signature components (user id and password) so that this other user could log in and change the rightful user password and then update the digital signature password, and then finally, while supplying all the credentials of the genuine owner, execute a signature. In CERF, these activities would be logged. Furthermore, the genuine owner would discover upon next attempted login that the system access password had been changed, then later, upon attempting an electronic signature, that the digital signature password had been changed. This would, presumably result in an investigation which would uncover the series of events and co-conspirators who enabled a fraudulent signature. It is the client's responsibility to protect and not share user passwords</p>
	<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</p>	Not Applicable	<p>Use and maintenance of biometric devices and software is outside the scope of the CERF system. Rescentris will advise its clients on the use of such methods for signatures, and may offer customized solutions for use of biometrics for electronic signatures.</p>
11.300	<p>Controls for identification codes/passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include</p>	CERF is Compliant	<p>CERF provides robust controls for use of identification codes/passwords in electronic signatures. These controls ensure the security and integrity of digital signature identification components in CERF.</p>
	<p>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.</p>	CERF is Compliant	<p>Uniqueness of each user id and password combination is enforced – no two individuals may have the same user id in CERF. CERF business policies also control the required complexity of the password, such as password length and the number of non-alphabetic characters required.</p>
	<p>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</p>	CERF is Compliant	<p>Password aging is fully supported by CERF. System business policies specify the frequency of required password renewals (every thirty days is a common setting). The user is first challenged to re-enter the current password before submitting a new password that must be different, meet organizational requirements for password complexity, and be entered twice identically in order for the password to be accepted.</p>
	<p>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.</p>	Not Applicable	<p>CERF does not use identification devices. However, the CERF administrator has authority to disable user accounts and to reset passwords. Users are required to modify their passwords immediately on login following a password reset.</p>

	<p>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.</p>	<p>CERF is Compliant</p>	<p>CERF offers several transaction safeguards to prevent unauthorized use, or attempted use, of the software. CERF can be set by the administrator to disable an account after a series of three incorrect logins (for example, three attempts with the wrong password). For security, only the administrator can re-enable the account for the genuine owner. Administrators can also specify a time-out period of inactivity after which a log-out is forced automatically by the system; after this, a user must login again with user id and password to create a new user session. A common time-out setting is thirty minutes. If a user is known to be gone for a long period, the account can be temporarily inactivated by the administrator, thus preventing any system access or electronic signatures associated with the user id of that individual. As another safeguard, CERF prevents any user from having more than one active session at a given time. If a user logs into CERF successfully, then goes to another computer and attempts to login, the individual is informed that there is already an active session at another (named) IP address. They can choose to log onto a new CERF session, which after proper credentials forcibly closes the previous session, or they can return to the other computer. All of these transactions are logged and available for monitoring and reporting by the administrator, who can investigate any unauthorized CERF use or attempted use, and can present these reports to organizational management.</p>
	<p>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.</p>	<p>Not Applicable</p>	<p>CERF user authentication does not use devices or tokens for user identification. Rescentris does recommend periodic verification of system security and documentation of testing practices and results. (Rescentris performs these tests with all new updates to the CERF software system before release.) If clients desire to use identification devices, Rescentris will offer consulting and customization services. Periodic testing after initial CERF deployment is dependent upon the operational controls and procedures established at the client.</p>