Document Control & 21 CFR Part 11

Some areas of the laboratory (especially blood banking) may be required to meet 21 CFR Part 11 requirements regarding electronic signatures. Document Control from MediaLab can help your laboratory address 21 CFR Part 11 requirements.

Subpart A General Provisions

This part lays out general definitions and terminology covered in 21 CFR Part 11, as well as the FDA's powers and responsibilities in this area. No specific requirements applicable to Document Control are introduced here.

Subpart B Electronic Records

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and 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:

21 CFR Part 11 Regulation	MediaLab's Capability	Subscriber's Steps to Address
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Provides step-by-step validation plan to subscribers.	Follow steps in validation plan and document their completion.
(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.	Displays documents in a human readable form on-screen. Provides documents in electronic form for download to authorized users. Allows authorized users to print controlled and uncontrolled paper copies.	Automatic
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are stored on redundant secure servers, backed up daily, and backups are provided to	Download backup file on a regular basis.

21 CFR Part 11 Regulation	MediaLab's Capability	Subscriber's Steps to Address
	subscribers for download	
(d) Limiting system access to authorized individuals.	Restricts access to users with established usernames and passwords	Ensure that access to given only to appropriate individuals.
(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.	Automatically records all actions taken by users and by the system. Actions are recorded in a permanent audit trail. Each action is time-stamped and cannot be altered or removed. Full audit trail is available to authorized users at any time.	Automatic
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Requires documents to pass through appropriate stages (editing, review, approval) before being made available to employees. Routes documents through applicable approval processes.	Automatic
(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.	Restricts access to documents and functions based on permissions granted to a user. User must be identified by username and password upon login; must identify with PIN prior to any signature.	Establish appropriate permissions within the system. Add or remove permissions as personnel and responsibilities change.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Requires username and password to authorize entry. Logs out users after set period of inactivity.	Complete validation plan. Ensure that users' computers are free from malware.
(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.	Provides CVs for key MediaLab personnel upon request. Provides user's guide, "Get started" wizard, training documents, and system help to guide users.	Evaluate employees' education, training, and experience.

21 CFR Part 11 Regulation	MediaLab's Capability	Subscriber's Steps to Address
(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.	n/a	Develop policies and procedures that reflect user responsibilities and requirements. Store these documents within Document Control.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Provides updated user's guide and release notes for system updates.	Review documentation and release notes for updates. Repeat validation after system updates to ensure proper operation.

Sec. 11.30 Controls for open systems.

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.

MediaLab Document Control is considered a closed system. This section is not applicable.

Sec. 11.50 Signature manifestations.

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer;	Included	Automatic
(2) The date and time when the signature was executed; and	Included	Automatic
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Included	Automatic
(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).	Included	Automatic

Sec. 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.

Signatures executed in MediaLab are permanently linked to the document and version that has been signed. The signatures cannot be edited, duplicated, or removed in any way.

Subpart C Electronic Signatures

Sec. 11.100 General requirements.

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Ensures uniqueness of signatures by irrevocably linking them to unique usernames, passwords, and PINs	Automatic

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(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.	n/a	Verify employee identity before distributing system credentials
(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.	n/a	Develop organizational policy / procedure and collect certifications as needed.
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.	n/a	Mail certification in paper form to specified address.
(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.	n/a	Develop organizational policy / procedure and collect certifications as needed.

Sec. 11.200 Electronic signature components and controls.

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	Requires three distinct components: username, password, and PIN.	Require each signer to create PIN (under "Home" tab).
(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.	Requires user to identify himself with username and password upon logging in to the system and after period of inactivity.	Automatic
(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.	Requires user to identify himself using PIN number before executing each signature.	Automatic
(2) Be used only by their genuine owners; and	Enforces uniqueness of username and ensures identity of genuine user by verifying password and PIN	Automatic
(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.	Does not permit an electronic signature to be used by anyone other than the genuine owner under any circumstance.	Automatic
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Does not use electronic signatures based on biometrics	n/a

Sec. 11.300 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:

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(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.	Ensures that usernames are unique to individuals and cannot be repeated. No two individuals can have duplicated identification codes.	Automatic
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Provides mechanism for periodic password expiration.	Establish time period for password expiration (under "Users" tab).
(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.	Provide mechanism to partially to completely revoke access for individual users.	Partially or completely revoke access for users when necessary.
(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.	Reports failed login attempts to genuine account holder, administrative users in the subscription, and MediaLab system support staff.	Automatic

21 CFR Part 11 Regulation	MediaLab's Capability	Steps to Address
(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.	Does not use these devices.	n/a

Last revision: December 20th, 2012