University of Michigan Health System
Compliance Checklist for 21 C.F.R. Part 11: FDA Electronic Records Mandates

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:

Subpart B Electronic Records Closed Systems Standards	Compliant?	Comments
11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	☐ Complete ☒ Partial ☐ None	1) The MCIT Change Management policy 02-003-001 requires that changes made to production systems will be managed. There are published change management processes for MCIT supported systems that reduce the risks for the confidentiality, integrity and availability of electronic information. CareWeb code changes follow a change management process and are documented using JIRA. The integrity and accuracy of Careweb data is ensured by audit logs/trails and through verification and testing by the CDR and QA teams. 2) The Quality Assurance team has 400 reuseable actions with 100 scripts that are run automatically on Mercury tools and used for functional and regression testing. The scripts are updated on a quarterly basis. 3) An audit log tracks all sign-ons of users (non-technical staff) to a hundredth of a second in the CareWeb system.
11.10(b) 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.	☒ Complete ☐ Partial ☐ None	
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	☒ Complete ☐ Partial ☐ None	
11.10(d) Limiting system access to authorized individuals.	☐ Complete ☒ Partial ☐ None	Access is role based and time limited. Accounts are provisioned and deprovisioned centrally. Currently all mainframe users have access by default. A change will be implemented in August/September to eliminate this default at which time we will consider this "complete".
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.	☒ Complete ☐ Partial ☐ None	
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	☒ Complete ☐ Partial ☐ None	Required and implemented for functions: Create Document, Edit / Sign
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.	☐ Complete ☒ Partial ☐ None	Access is role based and time limited. Accounts are provisioned and deprovisioned centrally. Currently all mainframe users have access by default. A change will be implemented in August/September to eliminate this default at which time we will consider this "complete".
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.	☐ Complete ☐ Partial ☐ None	N/A for our environment in that the source of commands or data is not relevant to establishing authenticity.

	☒ N/A*	According to the preamble, a given procedure or control is not intended to apply in all cases, the language of the rule so indicates, and 11.10(h) is one of those cited in this regard.
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.	☒ Complete ☐ Partial ☐ None	
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.	☒ Complete ☐ Partial ☐ None	
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.	☒ Complete ☐ Partial ☐ None	

Compliance Checklist for 21 C.F.R. Part 11: FDA Electronic Signatures Mandates

Subpart C - Electronic Signatures Standards		Compliant?	Comments
Signed electronic records must 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; and (3) the meaning (such as review, approval, responsibility, or authorship) associated with the signature.		☒ Complete ☐ Partial ☐ None	Compliant for (1) and (2) at least. (3) Sequencing of workflow indicates meaning.
The items identified above are subject to the same controls as for electronic records and are be included as part of any human readable form of the electronic record (such as electronic display or printout).		☒ Complete ☐ Partial ☐ None	
Electronic signatures and handwritten signatures executed to electronic records are 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.		☒ Complete ☐ Partial ☐ None	
Each electronic signature is unique to one individual and may not be reused by, or reassigned to, anyone else.		☒ Complete ☐ Partial ☐ None	
Identity verification is performed prior to establishing, assigning, certifying or otherwise sanctioning individual electronic signatures.		☒ Complete ☐ Partial ☐ None	
Written certification to FDA per regs that electronic signatures are intended to be the legally binding equivalent of traditional handwritten signatures. Ability to provide FDA, upon request, additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.		☒ Complete ☐ Partial ☐ None	
Signatures Not Based on Biometrics 11.200(a)	(1) Must employ at least two distinct identification components such as an identification code and password - (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. - (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.	☒ Complete ☐ Partial ☐ None	
	(2) Must be designed to ensure no use by anyone other than genuine owners, and in fact must be used only by genuine owners.	☒ Complete ☐ Partial ☐ None	
	(3) Must be administered and executed to ensure that attempted use by anyone other than genuine owner requires two or more people.	☐ Complete ☒ Partial ☐ None	Two factor authentication is used Unique name is public. Password reset process requires correct response to challenge questions.
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.	☐ Complete ☐ Partial ☐ None ☒ N/A*	
Controls for Electronic Signatures Based on ID Codes /	(a) Must maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	☒ Complete ☐ Partial ☐ None	
	(b) Must ensure that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such	☒ Complete ☐ Partial	

Passwords 11.300	events as password aging).	☐ None	
	(c) Must follow 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 issue temporary or permanent replacements using suitable, rigorous controls.	☒ Complete ☐ Partial ☐ None	
	(d) Must use transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and immediately report any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	☒ Complete ☐ Partial ☐ None	
	(e) Must conduct 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 inappropriately altered.	☐ Complete ☐ Partial ☐ None ☒ N/A*	

*11.10(f) N/A items: This is the information from the Federal Register, page 13444:

The agency advises that, where a given procedure or control is not intended to apply in all cases, the language of the rule so indicates. Specifically, use of operational checks (§ 11.10(f)) and device checks (§ 11.10(h)) is not required in all cases. The remaining requirements do apply in all cases and are, in the agency's opinion, the minimum needed to ensure the trustworthiness and reliability of electronic record systems. In addition, certain controls that firms deem adequate for their routine internal operations might nonetheless leave records vulnerable to manipulation and, thus, may be incompatible with FDA's responsibility to protect public health. The suggested revision would effectively permit firms to implement various controls selectively and possibly shield records from FDA, employ unqualified personnel, or permit employees to evade responsibility for fraudulent use of their electronic signatures.