SUBJECT: 21 CFR Part 11 compliance statement regarding Labmatrix

DATE: October 30, 2015

Labmatrix has been certified by the Center for Cancer Research (CCR) of the National Cancer Institute (NCI) as being compliant with 21 CFR Part 11¹.

21 CFR Part 11 applies to systems which maintain electronic records which are created, modified, maintained, archived, retrieved, or transmitted under records requirements set forth by the Food and Drug Administration (FDA). As it maintains electronic records of data that is part of FDA-regulated clinical studies, Labmatrix is such a system, and is maintained in strict compliance with 21 CFR Part 11 regulations, specifically those encompassing “closed” systems as defined by 21 CFR Part 11.

The current FDA guidance on 21 CFR Part 11² delineates the Agency’s recommendations for specific compliance criteria; by these criteria, as well as a reading of 21 CFR Part 11 itself, CCR has deemed Labmatrix to be compliant. Among other controls and requirements, Labmatrix adheres to the specific list of controls and requirements deemed to be within the FDA’s enforcement interest:

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- appropriate controls over systems documentation

Labmatrix also undergoes continuing Security Accreditation & Authorization (SA&A) assessments as part of its operations and maintenance.

CCR recognizes that compliance with 21 CFR Part 11 is a continuous process, requiring ongoing attention as systems undergo maintenance and as Agency interpretation evolves.

Jeff Shilling  
Chief of IT & Infrastructure Services, NCI CBIIT

Jason Levine  
Labmatrix System Owner, NCI CCR


Control

11.10 $(a)$ Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

full

LM can fully audit all data related and server related events, as can the OS and database.

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.

full

Records can be generated/exported via LM itself via multiple mechanisms, and API tools can also retrieve any and all LM data.

11.10 $(c)$ Protection of records to enable their accurate and ready retrieval throughout the records retention period.

full

LM data is fully backed up according to NCI CBIIT data protection standards.

11.10 $(d)$ Limiting system access to authorized individuals.

full

LM access is strictly and broadly governed by roles based permissions assigned within the system by authorized system administrators. Account passwords must be changed according to NIH standards, and unsuccessful login attempts result in account deactivation.

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.

full

Two different levels of audit logs are maintained for all data activity within LM, timestamped and with detail all the way down to the field change level.

11.10 $(f)$ Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

full

LM itself provides sequence based enforcements, as do external applications which run into the LM application software environment.

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.

full

Highly granular roles based permissions govern all access to LM, including read access, write/modification access, and search/query access.

11.10 $(h)$ Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source, access, and security of the origin of input or operational instruction.

N/A

LM training is provided to all users; SOPs are developed in concert with users for any specific workflows or data management needs.

11.10 $(i)$ Use of system checks to ensure the validity of the source of data input or operational instruction.

N/A

LM is not used for electronic signatures.

11.10 $(j)$ Use of system checks to ensure that all data input or operational instruction are usable, valid, and legal.

N/A

LM is not used for electronic signatures.

11.10 $(k)(1)$ Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

full

SOPs govern the ongoing development of LM and LM related functionality; all code is developed with full source control and code revisioning, all issue management is documented in an issue tracking system, and major system upgrades are fully documented by the vendor.

11.10 $(k)(2)$ Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and change maintenance.

full

SOPs are written and approved for this system, including change management and incident reporting.

11.10 $(l)$ Use of appropriate controls over systems documentation including: Adequate controls over access to, and use of, the subject electronic records.

full

SOPs are written and approved for this system, including change management and incident reporting.