DOMINO

Domino Data Lab – Statement on GxP Compliance

May 26, 2023

				Met By		
Area	**Regulation Summary**	**Regulation Description**	**Regulation**	**Domino**	**Customer**	**Domino Provides**
Validation	Systems should be validated for regulated use.	Systems must be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	21 CFR Part 11	x	x	Domino provides the functionality required for regulated use, such as control, versioning and audit trails. Domino validates its functionality, without a stated intended purpose. The recent FDA guidance requires that the functionality required for intended regulated use be validated specifically with that intent documented. Since the customer decides on the intended use, the customer must validate the functionality specifically required for that intended use. Guidelines also suggest a risk-based approach to testing, and Domino's Validation Package will provide the documented scope of testing it has performed.
Risk Management	Organizations should establish processes for regular audit trail review.	"Systems typically include many metadata fields and audit trails. It is expected that during validation of the system the organization will establish – based upon a documented and justified risk assessment – the frequency, roles and responsibilities, and the approach used to review the various types of meaningful metadata, such as audit trails."	WHO Annex 5	x		Domino provides three important features to enable customers to meet this need: 1) A Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. 2) A robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. 3) An activity report of the activities within a project. These allow the customer to establish and document an audit trail review process.
Risk Management	Organizations should perform regular risk-based reviews of metadata and audit trails.	Annex 5 requirements for a regular risk-based review of meaningful metadata and audit trails that is fit for use with regulated data.	WHO Annex 5	x	x	With respect to data privacy and ensuring that only the properly authorised individuals have had the correct level of access to the data, Domino's Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. With respect to the creation, deletion, and modification of data in Domino, this is done programmatically, via code (i.e. software) which the customer has developed and/or validated, owns, and executes in Domino. The execution of code is in the form of a Domino Job. Domino provides a robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. This report is available through the Domino user interface as well as API. Domino also provides an activity log of the activities which have occurred within a project. The customer must include a risk based review of the information provided by the Domino system.
Risk Management	Organizations should establish separation of duties and limit enhanced system and security access permissions.	Appropriate separation of duties should be established so that business process owners, or other users who may have a conflict of interest, are not granted enhanced security access permissions at any system level (e.g. operating system, application and database). Further, highly privileged system administrator accounts should be reserved for designated technical personnel, e. g. information technology (IT) personnel, who are fully independent of the personnel responsible for the content of the records, as these types of accounts may include the ability to change settings to overwrite, rename, delete, move data, change time/date settings, disable audit trails and perform other system maintenance functions that turn off the good data and record management practices (GDRP) controls for legible and traceable electronic data. Where it is not feasible to assign these independent security roles, other control strategies should be used to reduce data validity risks. To avoid conflicts of interest, these enhanced system access permissions should only be granted to personnel with system maintenance roles (e.g. IT, metrology, records control, engineering), that are fully independent of the personnel responsible for the content of the records (e.g. laboratory analysts, laboratory management, clinical investigators, study directors, production operators and production management). Where these independent security role assignments are not feasible, other control strategies should be used to reduce data validity risks.	WHO Annex 5	x	x	Domino provides a System Admin role. Currently, for customer hosted deployments of Domino, the actions performed by a System Admin must follow the customer's SOP for change control, without dependency on a Domino system audit trail report of these actions. For Domino Cloud for Life Sciences, Administrative functions follow a change contol SOP. A feature to extract an audit trail report of these actions is being prioritized in the product roadmap for delivery.
Personnel Training	Personnel with enhanced access permissions should be trained in data integrity principles.	It is particularly important that individuals with enhanced access permissions understand the impact of any changes they make using these privileges. Personnel with enhanced access should therefore also be trained in data integrity principles.	WHO Annex 5	x	x	Domino Cloud for Life Sciences is audit ready, and system administrators with enhanced permissions are trained. Additionally, System administrators are not able to access data owned by users unless they have been granted permission. For Domino's customer-hosted implementation, it is the customer's responsibility to train the system administrators with enhanced permission to the system in accordance with their standard operating procedures.
System Access	System maintenance roles should be separate from content management roles.	System maintenance roles (e.g. IT, metrology, records control, engineering), that are fully independent of the personnel responsible for the content of the records (e.g. laboratory analysts, laboratory management, clinical investigators, study directors, production operators and production management)	WHO Annex 5	x		Domino provides a System Admin role responsible for system maintenance, as well as content related roles, which are related to projects, data and code.

				Met By		
Area	**Regulation Summary**	**Regulation Description**	**Regulation**	**Domino**	**Customer**	**Domino Provides**
System Access	System access should be granted based on segregation of duties.	System access should be granted based on a segregation of duties and also the responsibilities of the investigator and the sponsor as outlined in ICH-GCP. For example, a person employed by the sponsor/CRO should not have edit rights to data entered into the eCRF by the investigator. Users with privileged or “admin access” typically have extensive rights in the system (operating system or application), including but not limited to changing any system setting (e.g. system time), defining or removing users (incl. “admin users”), activate or deactivate audit trail functionality (and sometimes even edit audit trail information) and making changes to data that are not captured in the audit trail (e.g. backend table changes in the database(s)). Users with privileged access should be sufficiently independent from and not be involved in the management and conduct of the clinical trial and in the generation, modification and review of data.	EMA Guideline on GCP	x		Domino provides a System Admin role responsible for system maintenance, as well as user roles which are related to content responsibility (code, data, projects). A System Admin does not have access to the code, data, or projects unless having been granted that access by the owner of those objects.
Data Transfer	Patient data should not be transferred outside the EU (except as defined in GDPR).	Patient data should not be transferred from the EU to a third party nation for processing without the appropriate agreements and safeguards as defined in GDPR Chapter 5.	GDPR	x	x	In the case that the appropriate agreements and safeguards have not been achieved, Domino Nexus capabilies allow for the processing of data to be performed without moving the data. Domino Nexus is Domino's hybrid implementation, which includes a control pane, hosted separately from data panes, which can be hosted on any Kubernetes enabled on prem infrastructure or cloud provider.
Data Access	Access to personal data should be limited to what is necessary for the specific purpose.	GDPR Article 25: Data Protection by Design and by Default: "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons."	GDPR	x		Domino provides an audit trail report per project, containing a timeline of who has been granted access to the data it contains. The audit trail report contains the ID of the user who performed the action, the date/time/timezone when the action was performed, the type of access granted or revoked, and the user id who has been granted/revoked access.
Audit Trails	Audit trails should include data on impacts to both data records and system environments.	“Audit trail. (1) (ISO) Data in the form of a logical path linking a sequence of events, used to trace the transactions that have affected the contents of a record. (2) A chronological record of system activities that is sufficient to enable the reconstruction, reviews, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.”	21 CFR Part 11	x		With respect to data privacy and ensuring that only the properly authorised individuals have had the correct level of access to the data, Domino’s Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. With respect to the creation, deletion, and modification of data in Domino, this is done programmatically, via code (i.e. software) which the customer has developed and/or validated, owns, and executes in Domino. The execution of code is in the form of a Domino Job. Domino provides a robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. This report is available through the Domino user interface as well as API. Domino also provides an activity log of the activities which have occurred within a project.
Audit Trails	Audit trails should include the reason for a change, and be regularly reviewed.	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	EudraLex Annex 11	x	x	With respect to data privacy and ensuring that only the properly authorised individuals have had the correct level of access to the data, Domino’s Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. With respect to the creation, deletion, and modification of data in Domino, this is done programmatically, via code (i.e. software) which the customer has developed and/or validated, owns, and executes in Domino. The execution of code is in the form of a Domino Job. Domino provides a robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. This report is available through the Domino user interface as well as API. Domino also provides an activity log of the activities which have occured within a project. These allow the customer to establish and document an audit trail review process.
Audit Trails	Organizations should use audit trails in applying controls to comply with rule requirements.	“The Agency intends to exercise enforcement discretion regarding specific part 11 requirements related to computer-generated, time-stamped audit trails (§ 11.10 (e), (k)(2) and any corresponding requirement in §11.30). Persons must still comply with all applicable predicate rule requirements related to documentation of, for example, date (e.g., § 58.130(e)), time, or sequencing of events, as well as any requirements for ensuring that changes to records do not obscure previous entries. Even if there are no predicate rule requirements to document, for example, date, time, or sequence of events in a particular instance, it may nonetheless be important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the records. We recommend that you base your decision on whether to apply audit trails, or other appropriate measures, on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety and record integrity. We suggest that you apply appropriate controls based on such an assessment. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation.”	21 CFR Part 11	x		With respect to data privacy and ensuring that only the properly authorised individuals have had the correct level of access to the data, Domino’s Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. With respect to the creation, deletion, and modification of data in Domino, this is done programmatically, via code (i.e. software) which the customer has developed and/or validated, owns, and executes in Domino. The execution of code is in the form of a Domino Job. Domino provides a robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. This report is available through the Domino user interface as well as API. Domino also provides an activity log of the activities which have occurred within a project.

				Met By		
Area	**Regulation Summary**	**Regulation Description**	**Regulation**	**Domino**	**Customer**	**Domino Provides**
Audit Trails	Organizations should provide FDA auditors with copies of electronic records in a common format.	“The Agency intends to exercise enforcement discretion with regard to specific part 11 requirements for generating copies of records (§ 11.10 (b) and any corresponding requirement in §11.30). You should provide an investigator with reasonable and useful access to records during an inspection. All records held by you are subject to inspection in accordance with predicate rules (e.g., §§ 211.180(c), (d), and 108.35(c)(3)(ii)). We recommend that you supply copies of electronic records by: - Producing copies of records held in common portable formats when records are maintained in these formats - Using established automated conversion or export methods, where available, to make copies in a more common format (examples of such formats include, but are not limited to, PDF, XML, or SGML) In each case, we recommend that the copying process used produces copies that preserve the content and meaning of the record. If you have the ability to search, sort, or trend part 11 records, copies given to the Agency should provide the same capability if it is reasonable and technically feasible. You should allow inspection, review, and copying of records in a human readable form at your site using your hardware and following your established procedures and techniques for accessing records.”	21 CFR Part 11	x	x	With respect to data privacy and ensuring that only the properly authorised individuals have had the correct level of access to the data, Domino’s Data Access Management Audit Report which shows who has been granted what access to what data at what point in time and by whom. With respect to the creation, deletion, and modification of data in Domino, this is done programmatically, via code (i.e. software) which the customer has developed and/or validated, owns, and executes in Domino. The execution of code is in the form of a Domino Job. Domino provides a robust audit trail of job executions which have changed data or generated an output. In addition to who executed the job at what point in time, this audit trail additionally provides details on the input data, code, environment (packages, etc.), output, and logs, including versions and change impact. This report is available through the Domino user interface as well as API. Domino also provides an activity log of the activities which have occurred within a project.
Audit Trails	Organizations should maintain records of processing activities as specified in GDPR Article 30.	GDPR Article 30: Records of Processing Activities: 1. Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). 2. Each processor and, where applicable, the processor’s representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller’s or the processor’s representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). 3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. 4. The controller or the processor and, where applicable, the controller’s or the processor’s representative, shall make the record available to the supervisory authority on request. 5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	GDPR	x	x	Domino provides the following capabilities which enable compliance without inhibiting the use of data: 1. Domino provides an Data Access Management audit trail report providing records of who has been granted what access to what data at what point in time and by whom. 2. Domino Nexus provides a mechanism for processing data without transferring it outside of the country.