COMPLIANCE TEAM

The *Definitive* Data Integrity Checklist

Directions: For each checklist item below, if the answer is "No," correction is recommended unless the organization can provide a justification.

General

- ☐ Has a formal data integrity training program has been established across the organization?
- ☐ Does the company have a policy for investigation of data integrity issues?
- ☐ Does Management support data integrity with programs such as an anonymous reporting system to report unethical behavior to company data governance officials?
- ☐ Is the state of Data Integrity discussed at Management Review meetings?
- ☐ Has a formal data integrity training program has been established across the organization?
- ☐ Do policies to mandate users to log off their systems when they plan to be away from their desks?
- ☐ Do policies mandate contemporaneous data entries? This includes prohibiting use of sticky notes for temporary data entry until it can be entered on the official record.
- ☐ Do policies specifically prohibit backdating/post-dating/pre-dating information (i.e. the date of document entry is the date that shows on the document entry date.)
- ☐ Does the company have policies pertaining to use of, and archive of e-mail communications that contain information pertinent to a quality decision affecting the product or process?
- ☐ Does company policy specify that electronic signatures and handwritten signatures are equivalent?
- ☐ Do policies mandate that IT system administrators be independent from operations taking place in the computerized system (i.e. System Admins report to IT, and not the production/QA department?)
- ☐ Is data security seriously considered, for example through an ethical hacking program, Phishing tests and awareness of spurious e-mail attachments?
- ☐ Are systems protected from access to/hacking from the Internet?
- ☐ Are procedures in place that mandate proper error correction of handwritten document entries, observing Good Documentation Practices?
- ☐ Does Management provide resources to ensure that all records, electronic and paper, are stored in secure, fire-safe locations?
- ☐ Are procedures in place to prohibit destruction of original data whether handwritten or electronic?
- ☐ If data are stored at a 3rd-party storage facility or on a "cloud," have Supplier Quality Reviews been performed to assure continued data integrity over the entire retention period for the data?
- ☐ Are GxP-relevant data archived according to the mandated data retention schedules?
- ☐ Are all data created (whether handwritten or computer-generated) attributable to the specific individual who generated it?
- ☐ Does the company keep a signature log to identify handwritten signatures that may not be readily attributable to the specific individual?
- ☐ Do all GxP-relevant data have a documented review by at least one individual other than the individual who created it?
- ☐ Do policies ensure that data integrity issues, if present are observable and evident to facilitate correction and prevention at the earliest possible opportunity?
- ☐ Do policies and procedures specifically prohibit write-overs, white-out, erasing, document shredding and other data obliteration methods?
- ☐ Is Data Integrity a checklist item for evaluation of raw material suppliers?
- ☐ Do policies and procedures and computerized systems specifically prevent write over of electronic data, for example, by replacing a file with a new file bearing the same filename or use of Recycle bin?
- ☐ Are page numbers identified by "Page *X* of *Y*" so missing pages of a record are immediately evident?

Administration

- ☐ Does an SOP define the process for removing roles/users from the system (e.g. after exit from the company, promotion, or move to a new role within the company)?
- ☐ Does an SOP mandate that all changes requiring Administrator access have a signed form (electronically or via handwritten signature) with approvals and justification for specified changes?
- ☐ Does the SOP for setup of user privileges provide a mechanism for tightly controlling the number of System Administrators?
- ☐ Is setup of users and privileges (i.e. creating/editing/modifying/deleting access) limited to the Administrator role?
- ☐ Is setup of group privileges limited to the Administrator role?
- ☐ Is setup of security settings (e.g. turning on/off security options, archival) in the software limited to the Administrator role?
- ☐ Are system administrators restricted from accessing records (other than read-only) in the system?
- ☐ Does each system have a defined inventory of system users, roles and permissions?

User/System Maintenance

- ☐ Does each system have an established SOP to define system use and maintenance?
- ☐ Is user access limited to users with accounts on a given system?
- ☐ Do procedures ensure that no individual can both write and edit the same data within a system?
- ☐ Does each system have a defined system owner(s) accountable for system maintenance, setup, identification of users, and data integrity?
- ☐ Do procedures govern assignment and approval of individuals to appropriate roles and permissions?
- ☐ Is a procedure in place to document a review the user roles and permissions and update at regular intervals (i.e. periodic user maintenance)?
- ☐ Do systems have a means of obtaining a list of users/roles to facilitate periodic user maintenance?
- ☐ Does each system have at least three user groups assigned (e.g. User, Supervisor, Administrator)?
- ☐ Are all available user groups defined in an SOP governing proper system access?
- ☐ Do records for user privileges and user groups reflect that the SOP for user access is being followed?
- ☐ Are managers' logins limited to data approval, not for data creation/alteration or administration functions?
- ☐ Are procedures in place to mandate a documented review of computer system audit trails at specified, regular intervals?
- ☐ Do change control procedures require written justification and approval for changes in software/firmware/operating system versions?
- ☐ Do procedures require justification and approval of administrative setting changes, (e.g. paths for file storage and enablement of audit trails)?
- ☐ Are administrative setting changes captured on the audit trail?
- ☐ Are users' access rights on the data system consistent with access rights on the client machine and/or server?

Access Control

- ☐ Do policies ensure that unique, individual logins be assigned for access to any GxP system?
- ☐ Do systems have a unique system login for each user having access?
- ☐ Whenever possible, is system data integrity designed into the system via access controls, rather than though process and procedure?
- ☐ Are controls in place for biometric system access, or, alternatively, to regularly update passwords?
- ☐ Are users restricted from full access to a given system (i.e. application, program files, and operating system) unless possessing a valid, user-specific username and password (or biometric control)?
- ☐ If biometric practices are not employed, do policies or electronic standards enforce a minimal level of password complexity?
- ☐ If biometric practices are not employed, are systems in place to automatically prompt for a change of password after a specified period of use?
- ☐ If biometric practices are not employed, do procedures specify never to share passwords and/or write them down?
- ☐ Do policies mandate that users to log off their systems when they plan to be away from their desks?
- ☐ Does a system time out after a period of inactivity, to confirm that the same user is on the system?

Export

- ☐ Are exported data only presented in a non-editable format?
- ☐ When exported data are used, are they authenticated to be a true copy of the original?
- ☐ When data are exported, is it evident that the data are copies, and not the original?
- ☐ When data are exported, does it contain the necessary data elements
  - Date/timestamp
  - Activity Completed
  - Individual performing the activity (e. g. username)

Audit Trails

- ☐ Does an audit trail exist for every GxP-relevant system?
- ☐ For systems with audit trail functions, is this functionality intact (i.e. not disabled)?
- ☐ If the system has electronic signature capability, does an audit trail track metadata for the electronic signature including the following:
  - Individual performing the electronic signature (e. g. username)
  - Meaning of the electronic signature
  - Date/Timestamp for the electronic signature
- ☐ Are audit trails for the system readily viewable (i.e. human-readable) by anyone with permissions to work in the system?
- ☐ Are audit trails for the system restricted from data alteration by anyone in the system?
- ☐ Has the data audit trail been validated to be a true representation of system activity?
- ☐ Does the audit trail record for any given activity contain the following data elements?
  - Date/timestamp
  - Activity completed
  - Individual performing the activity (e. g. username)
- ☐ To secure audit trail integrity, is access to date/time settings restricted to only users in the Administrator role?
- ☐ Are *all* GxP-relevant data creation/update/deletion activities recorded on an audit trail?

Validation

- ☐ Do User Requirements for computerized systems specify the need to restrict users from the ability to alter records within the system?
- ☐ Has the system been validated to ensure that reports display user information and data accurately (i.e. true copy)?
- ☐ Do specification documents/DQ for electronic system include a supplier evaluation to ensure that data integrity is designed into the system from the vendor
- ☐ Does the system validation verify all workflow paths that could be used for managing GxP data?
- ☐ Does validation of the system verify proper administrative settings, such as paths for file storage, and enablement of audit trails?
- ☐ Does system validation comprise IQ, OQ, and PQ (or PV/TMV)?
- ☐ Does a policy mandate a validation assessment of GxP-relevant systems per 21 CFR Part 11?
- ☐ When a Part 11 gap is identified, does the policy mandate that the system be remediated into Part 11 compliance before it is validated and used for GxP purposes?
- ☐ If data backup is performed using external drives/devices, are these devices qualified/validated to provide an accurate true copy of data?
- ☐ Is the backup version of the audit trail validated to be unaltered (i.e. true copy) in human-readable format?
- ☐ Does validation of the system record all applicable software/firmware/operating system versions for the various system elements?
- ☐ When software/firmware/operating systems are updated, is the system revalidated to ensure that these changes did not alter the accuracy or true copy of data?
- ☐ Does validation cover verification of data reduction calculations, to ensure correct results?
- ☐ When relocating computerized systems, is a validation assessment conducted to ensure that data integrity is not affected (e.g. new Ethernet connection may not support data archive functions.)?
- ☐ Does the system have a validated method for automatic daylight savings time updates?
- ☐ When temporary roles are assigned during system validation, does the validation package ensure that the temporary roles are revoked after validation execution and turnover for GxP use?
- ☐ Has the data backup process been validated to ensure that the backed-up data are a true copy?
- ☐ Has the audit trail been validated to be uneditable by users at any access level?
- ☐ Does the company have a validation plan and budget in place for remediation of legacy systems for data integrity improvements?
- ☐ Has the company established, and adhered to a schedule for periodic validation reviews for systems that generate, manipulate, maintain and archive data?
- ☐ Are system data integrity concerns reviewed during periodic validation reviews for legacy systems?

Data Maintenance

- ☐ Are data are regularly reviewed in storage/archive locations to ensure that they are free from damage, loss, and deterioration?
- ☐ Are electronic systems networked in order to facilitate backup of data to a secure server?
- ☐ Are data authenticated to ensure it is a true copy for its entire lifecycle (i.e. from raw data creation, data calculation/reduction through data archival/storage, and retrieval from backup)?
- ☐ Does a given system have autosave functionality, to prevent data loss, with an established file path in a location where the user cannot alter the data?
- ☐ Do systems restrict users from copying data from the established file path to other locations?
- ☐ Do policies and procedures discourage the use of "hybrid" systems, and prefer using the electronic raw data as the official data of record?
- ☐ If the system is used as a "hybrid" system, is a procedure in place to authenticate the paper record against the electronically-generated results?
- ☐ If the system is used as a "hybrid" system, do policies still require maintaining the original electronic data so the integrity of such data can be evaluated for data integrity in the future?
- ☐ Are users restricted from altering data files (i.e. copy, delete, modify) via the operating system, "C:" drive, or independently through any other means, such as the application software or database?
- ☐ Are all elements of the data management system within their normal, serviceable lifespan such that all data system elements properly communicate without obsolete elements that affect critical functions such as storage, retrieval, or translation of electronic data into human-readable format?
- ☐ When data need to be changed, does the system prompt the user to provide a justification for changing the defined data element(s)?
- ☐ When data need to be changed, are changes reviewed and approved by at least one individual not directly involved in the generation of the data element(s)being changed?
- ☐ Does the system reject import of files created or modified from outside a given system?

Backup

- ☐ Are GxP data backed up at regular intervals (e.g. weekly)?
- ☐ Is the metadata (including audit trail) also backed up at regular intervals?
- ☐ Was a folder structure established for location of all backed-up data?
- ☐ If the data backup process is automatic, has this automated function been validated to ensure that the backups occur at the designated frequency?
- ☐ If the data backup process is automatic, has a notification system been validated to ensure that an administrator is notified if the data backup process fails?
- ☐ If the data backup process is automatic, are procedures in place to ensure that an administrator regularly documents that the data backups were confirmed successful, and if not, acts to ensure proper data backup?
- ☐ If a data backup is performed manually, is a record created to identify the individual performing the data backup, the date backup was performed, and the data affected by the backup?
- ☐ If data backup is performed manually using external drives/devices, is physical access to these devices controlled?
- ☐ If data backup is performed manually using external drives, are these devices properly inventoried?
- ☐ Are data backup configuration/performance restricted only to individuals who had no input on generation/approval of the data being backed up?
- ☐ Once data are backed-up, are individuals restricted to read-only access to the data backup?

QC/Instrumentation

- ☐ Are polices in place to prohibit "testing into compliance" without investigation of OOS events?
- ☐ Are GxP (QC and manufacturing) records reviewed in full by the Quality Unit before release?
- ☐ Do SOPs require the record to identify the individual involved in making the quality decision resulting from evaluation of the QC data?
- ☐ Do training programs/records ensure that all analysts interpret QC data in a consistent manner?
- ☐ Does the company mandate that OOS investigations be conducted on instrumentation meeting data integrity standards as rigorous as those employed in the QC lab?
- ☐ Does the system and/or associated procedures require the user to associate all aborted operation data or orphan data to a formal record?
- ☐ Are users responsible for verification of output records trained in data review in the system, ensuring that all aborted operation data and orphan data are included in the formal record?
- ☐ Are data calculations supporting GxP activities validated (or verified by a second individual) before their use in formulating a quality decision?
- ☐ When an operation or experiment is aborted mid-execution, does the system prompt the user to provide a justification for failure to proceed with the operation?
- ☐ Are approved, programmed, non-editable protocols and/or data templates installed on instrumentation to minimize variability between test procedures and analysts, thus ensuring data are consistent from one analysis and the next?
- ☐ If data can be reprocessed (i.e. dynamic systems) does the audit trail track all reprocess events?
- ☐ If data can be reprocessed (i.e. dynamic systems) do procedures mandate review of all reprocessed data before release?
- ☐ If data can be reprocessed (i.e. dynamic systems) do procedures mandate review of both the raw data and the processed data before release?
- ☐ If data can be reprocessed (i.e. dynamic systems) do procedures mandate secondary approvals whenever the data undergo more than one (initial) processing step?
- ☐ Are changes to GxP records (including invalidation of results) justified and then approved by managers who are not directly involved in creating and/or modifying the data?
- ☐ For chromatography systems, does the quality system require secondary reviews/approvals whenever data are manually integrated?
- ☐ For chromatography systems, does a procedure clearly prohibit "test" or "trial" injections, or prospectively provide stringent criteria for times when such injections may be necessary?
- ☐ For GxP records that are created through visual inspection, such as plate counts or instruments without a printing application, do procedures mandate a secondary verification of data entries?
- ☐ Are procedures in place that mandate that the GxP record contain the complete history of results obtained through the analysis, including invalid and OOS data, not just the final result?
- ☐ Do established procedures ensure review, authentication, and commensurate quality review of audit trails for all GxP analyses prior to release?
- ☐ For chromatography systems, do procedures mandate secondary approvals when an atypical integration event is observed (e.g. tangential skims, exponential skims, droplines)?
- ☐ Does a procedure provide consistent integration interpretation criteria for any standard chromatographic test?
- ☐ Do chromatography procedures use a "Master" chromatogram on file as a standard?
- ☐ Are systems calibrated to bracket the full anticipated measurement range employed in analysis?
- ☐ Are validity checks for dynamic systems limited to analysis of known, approved reference materials for which the expected test results are well-established?