11 COMPLIANCE CHECKLIST

VERSION 1 – OCTOBER 2021

INTRODUCTION

21 CFR Part 11 is an FDA guidance that sets out how organizations operating in the United States can use electronic records and digital signatures in their quality management systems to replace paper-based documents and 'wet signatures'.

Any organization that uses quality management and needs to conform to FDA regulations, such as pharmaceutical and life sciences organizations, needs to be aware of 21 CFR Part 11, and be compliant.

This document takes you through 4 stages of compliance - with individual checklists for each.

PART 1. VALIDATION

- [ ] Is your existing system validated?
- [ ] Can you identify invalid or altered records?
- [ ] Are your records readily retrievable across their retention period?
- [ ] Can the system limit access to authorized individuals?
- [ ] Can a specific sequence of steps or events be enforced by the system (process control)?
- [ ] Are user based permissions possible for electronically signing records, altering a record, or performing other operations?
- [ ] Does the system make a provision for checking or restricting instructions and/or data from specific devices (such as scales or thermometers)?
- [ ] Is your training documented, including in-situ training for system users, IT support staff and developers?
- [ ] Are there written policies that make individuals fully accountable and responsible for actions determined by their electronic signatures?
- [ ] Is all distribution, access, and use of systems operation and maintenance documentation controlled?
- [ ] Is system data encrypted?
- [ ] Are digital signatures used?

COMPLIANCE CONSULTING

PART 2. AN AUDIT TRAIL FOR EVERY DOCUMENT

- [ ] Do you have a secure, tamper-proof audit trail that records the date and time of operator entries and actions that interact with electronic records?
- [ ] Does your system have version control - allowing access to previous, unaltered versions of information?
- [ ] Is the audit trail for an electronic record retrievable throughout the record's retention period?
- [ ] Is the audit trail comprehensive - including the User, all actions, links to edits and versions, a change log, and revision and change controls?
- [ ] Are audit trails available for review and interrogation by the FDA?
- [ ] Do signed electronic records contain:
  - The name of the signee
  - The date and time of signing
  - The type of signing (approval, review, etc.)
  - Is the above information displayed on all copies of the electronic record (digital and printed)?
- [ ] Are electronic signatures unique to a specific user or individual?
- [ ] Do user ever share electronic signatures?
- [ ] What additional authentication is performed to verify the identity of an individual before an electronic signature is used?
- [ ] When multiple signings are performed during a single session, what level of authentication is executed for each signing?
- [ ] Are signatures explicitly associated with their respective electronic records to ensure that they cannot be altered or otherwise transferred by ordinary means for the purpose of falsification?
- [ ] Does your formal change control procedure for system documentation maintain its own audit trail for all changes?
- [ ] How do you ensure non-biometric signatures are only used by their genuine owners?
- [ ] Is it possible to falsify an electronic signature? If so, how?

PART 3. COPIES OF RECORDS

- [ ] Is the system capable of producing accurate and complete copies of electronic records on paper?
- [ ] Is the system capable of producing accurate, complete and un-editable copies of records in electronic form? Can these be provided to the FDA for inspection and review?
- [ ] What established automated conversion or export methods (eg PDF, XML, SGML) is the system using?

PART 4. RECORD RETENTION

- [ ] Is the system able to force automatic password expiration and renewal?
- [ ] Is there a procedure for recalling authentication methods and passwords if a person leaves or is transferred?
- [ ] What is the procedure for electronically disabling an identification code or password if it is lost or compromised?
- [ ] What is the procedure for detecting unauthorized access attempts to the system?
- [ ] What is the procedure for informing security of unauthorized access attempts?
- [ ] What is the procedure for informing management of unauthorized access attempts?
- [ ] What is the procedure for reporting and managing a lost or stolen device?
- [ ] What is the procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?
- [ ] What controls exist for issuing temporary or permanent replacement devices?
- [ ] Is there initial and periodic testing of security tokens and cards?
- [ ] Does this testing check that for any unauthorized alterations?