21 CFR Part 11 Compliance Checklist

Part 1: Validation

- ❑ Is the system validated?
- ❑ Is it possible to discern invalid or altered records?
- ❑ Are the records readily retrievable throughout their retention period?
- ❑ Is system access limited to authorized individuals?
- ❑ If the sequence of system steps or events is important, is this enforced by the system (process control system)?
- ❑ Does the system ensure that only authorized individuals can use it, electronically sign records, alter a record, or perform other operations?
- ❑ If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weight scales, or remote, radio controlled terminals).
- ❑ Is there documented training, including on the job training for system users, developers, IT support staff?
- ❑ Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?
- ❑ Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?
- ❑ Is data encrypted?
- ❑ Are digital signatures used?

Part 2. An Audit Trail For Every Document

- ❑ Is there a secure, computer-generated, time-stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?
- ❑ Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?
- ❑ Is an electronic records audit trail retrievable throughout the record's retention period?
- ❑ Is the audit trail available for review and copying by the FDA?
- ❑ Does the audit trail include the User ID, sequence of events (in particular scenarios or instances), original and new values (Backups of any modified or deleted records), a change log, and revision and change controls?
- ❑ Do signed electronic records contain:
    - ❑ The printed name of the signer
    - ❑ The date and time of signing
    - ❑ The meaning of the signing (such as approval, review, etc.)

21 CFR Part 11 Compliance Checklist

- ❏ Is the above information shown on displayed and printed copies of the electronic record?

- ❏ Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?
- ❏ Is there a formal change control procedure for system documentation that maintains a time-sequenced audit trail for those changes made by the pharmaceutical organization?
- ❏ Are electronic signatures unique to an individual?
- ❏ Are electronic signatures ever reused by or reassigned to anyone else?
- ❏ Is the identity of an individual verified before an electronic signature is allocated?
- ❏ Is the signature made up of at least two components, such as an identification code and password, or an id card and password?
- ❏ Has it been shown that biometric electronic signatures can be used only by their genuine owner?
- ❏ When several signings are made during a continuous session, is the password executed at each signing? (Note: Both components must be executed at the first signing of a session.)
- ❏ If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?
- ❏ Are non-biometric signatures only used by their genuine owners?
- ❏ Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?

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 and complete copies of records in electronic form for inspection, review, and copying by the FDA?
- ❏ Is the system using established automated conversion or export methods (PDF, XML, or SGML)?

Part 4. Record Retention

- ❏ Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?
- ❏ Are procedures in place to ensure that the validity of identification codes is periodically checked?
- ❏ Do passwords periodically expire and need to be revised?
- ❏ Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?

21 CFR Part 11 Compliance Checklist

- ❏ Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?
- ❏ Is there a procedure for detecting attempts at unauthorized use and for informing security?
- ❏ Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?
- ❏ Is there a loss management procedure to be followed if a device is lost or stolen?
- ❏ Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?
- ❏ Are there controls over the issuance of temporary and permanent replacements?
- ❏ Is there initial and periodic testing of tokens and cards?
- ❏ Does this testing check that there have been no unauthorized alterations?