21 CFR part 11 compliance

PMA.core was developed with the FDA 21 CFR part 11 guidelines in mind.

Our software adheres to the following principles:

- Data will be formatted to allow transfer to another system for long-term storage in a common portable format either during the life of the system or after the system is retired
- The system will contain detection mechanisms for invalid field entries, values out of range, and blank fields if entry is required
- It will be possible to provide regulatory agencies with both human-readable and electronic copies of the records, including metadata. It will be possible to transfer data in a human readable format onto transportable media such as PDF, XML, SGML. The system must allow that the copying process produces copies that preserve the content and meaning of the records
- If it is important to system functionally that steps be performed in a specified order, the system will contain a mechanism to ensure that actions are performed in the correct sequence (in case of sequenced steps)
- The system will contain an automatically generated audit trail function for all process significant and GxP critical events and allow audit trails on tables and individual records
- The audit trail data will be read-only
- It will be impossible to disable the audit trail function
- The system will prevent the accidental or intentional modifications or deletion of audit trail files
- It will be possible to generate a report to view which data in the record has been modified
- A mechanism will be in place to detect and report any attempts of unauthorized use immediately to the customer
- The audit trail will record: user name, data and time (h/min/sec) of the event using local data and time of the host system, indication of the type of event: record creation/modification/deletion or approval, in case of modification/deletion: old value and new value, reason of change (if applicable)
- A specific link must be in place to trace the audit trail data to the associated electronic record(s) itself
- The system will not allow changes in date and time by the user
- The system date and time will be periodically checked and corrected. The system will support time synchronization
- The electronic audit trails will be readily available for review
- The system will be protected against unauthorized use
- Security will consist of at least two elements (e.g. login ID and password) in case of non-biometric security
- The system must enforce and automatic log-out after a defined period of no activity
- The system will allow the specification of different levels of access (e.g. user, administrator)
- The system will detect security violations and produce an alarm or warning message
- Controls will be in place to ensure that no two (2) individuals can have the same combination of identification code and password
- If a password is not issued privately (i.e. the password issuer knows the password), the user will immediately reset their password

Wikipedia has more background on this topic.