WHITE PAPER

Agiloft

# AGILOFT COMPLIANCE WITH CFR 21 PART 11

# Table of Contents

# AGILOFT COMPLIANCE WITH CFR 21 PART 11

Almost all industries depend upon software for the efficient, auditable and reliable execution of their business processes. For most companies subject to FDA regulation, this requires compliance with CFR 21 Part 11 if these processes involve the use of electronic signatures on data required to be maintained by the FDA predicate rule or used to demonstrate compliance with such a rule.

This paper provides an overview of the rule and describes how Agiloft supports it.

## Overview

**According to the FDA's definition**, "an electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."

As stated by the FDA in its guidance documents, CFR 21 Part 11 ensures companies "employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."

These predicate rules address the research, production and control of FDA regulated articles such as manufacturing/laboratory processes, clinical/pre-clinical research, adverse event reporting, product tracking and marketing submissions and reports.

Fulfilling these requirements is aided by a system that meets the following criteria:

## Verifiable Support for End-User Requirements

As the FDA notes in its guidance documents on CFR 21 Part 11, "establishing documented end user (i.e., a person regulated by FDA) requirements is extremely important for computer systems validation. Without first establishing end user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them. Once you have established the end user's needs and intended uses, you should obtain evidence that the computer system implements those needs."

This requirement is greatly facilitated by a system that is not only easily configurable to end-user requirements, but fully exposes how those requirements have been met. For example, the tools for setting access permissions and configuring workflows should be driven entirely through the browser and provide a visual representation of the resulting configuration. If the configuration depends upon custom programming, it becomes opaque to everyone except a programmer skilled in that language and only such a programmer can certify that it implements the user needs correctly or make necessary adjustments.

## Electronic Signature Support

The system must support electronic signatures at multiple levels — it should not only enforce the use of electronic signatures when changing controlled records, but the presence of these guards should be easily verifiable and the use of each signature fully auditable.

## Precise Access Controls

User access to individual records and to particular fields within those records must be precisely controlled by security groups. In addition, the system should be capable of restricting access based upon IP address and should support integration with biometric controls.

## Change Tracking and History

Every change to each record must be recorded, with a timestamp showing who made the change, what they changed and when the change occurred. The system should be capable of displaying what the entire record looked like at any point in the past. Further, the solution must make it possible to capture and collate data, such as who logged in, what IP address they came from, what records they edited, etc.

## Auditability

The system must be auditable in multiple senses. It must make it easy to show an auditor what a defined business process is, how the system enforces the process, and how the process has been followed in any particular instance.

## Security

The software and any hosting infrastructure should be subject to regular security audits from an independent third party and the results of that audit should be made available upon request.

# 21 CFR PART 11 COMPLIANCE MATRIX

The following tables describe how Agiloft supports compliance with 21 CFR Part 11.

As noted by the FDA, "Electronic record and electronic signature systems consist of both manual procedural controls and technical controls implemented through computer systems", so while the use of compliant software is a necessary condition for Part 11 compliance, it is not a sufficient condition, because several aspects of the rule depend upon the organization following appropriate procedures. These are indicated in this matrix with the response, "The customer is responsible for adhering to this requirement.

The term "Acknowledged" is used to indicate areas where the recommendation has been read and understood, but there is no specific functionality required on the part of the software.

## Subpart A – General Provisions

| Sec. 11.1 Scope. | Agiloft Compliance |
|---|---|
| **(a)** The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. | Agiloft supports electronic signatures through integration with DocuSign. Further, it positively identifies the user through a unique username and password combination. This information is controlled and centrally managed via a license server. LDAP integration allows the administrator to use LDAP to replace/supplement the built-in user management. |
| **(b)** This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means. | Acknowledged |

| Sec. 11.1 Scope. | Agiloft Compliance |
|---|---|
| (c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997. | Acknowledged |
| (d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required. | Acknowledged |
| (e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection. | Agiloft shall comply with any request to inspect its hardware, software, controls and attendant documentation by the FDA. |
| (f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.<br>[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004] | Acknowledged |

| Sec. 11.2 Implementation. | Agiloft Compliance |
|---|---|
| (a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met. | Acknowledged |
| (b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: | Acknowledged |
| (1) The requirements of this part are met; and | Acknowledged |

| Sec. 11.2 Implementation. | Agiloft Compliance |
|---|---|
| (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission. | Acknowledged |

| Sec. 11.3 Definitions. | Agiloft Compliance |
|---|---|
| (a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. | Acknowledged |
| (b) The following definitions of terms also apply to this part: | Acknowledged |
| (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). | Acknowledged |
| (2) Agency means the Food and Drug Administration. | |
| (3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. | Agiloft includes API's to integrate with biometric systems. As it is a software product, it does not include the use of specific biometric hardware. |
| (4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. | Agiloft can be configured as either an open or closed system. |

| Sec. 11.3 Definitions. | Agiloft Compliance |
|---|---|
| **(5)** Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. | Agiloft uses a set of rules based on security group settings that uniquely identifies the user from their username and password combination. The internal security settings in these tools determine the access and privileges of the signed in user. The transfer of all information is protected through cryptography. |
| **(6)** Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. | Acknowledged |
| **(7)** Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. | Acknowledged |
| **(8)** Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. | Agiloft includes API's to integrate with biometric systems. As it is a software product, it does not include the use of specific biometric hardware. |
| **(9)** Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system. | Agiloft can be configured as either an open or closed system. |

## Subpart B – Electronic Records

| Sec. 11.10 Controls for closed systems. | Agiloft Compliance |
|---|---|
| Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | Agiloft supports controls to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records as detailed below. |
| **(a)** Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | In addition to access controls that determine who can view or modify individual records or fields within records, Agiloft provides History tracking that shows exactly what changes particular users made to each record, and a snapshot of the entire record before and after each change. In addition, audit logs may be configured to track the IP address of the user who altered or viewed each record and rules may be configured to flag records as invalid based upon criteria defined by the administrator. |
| **(b)** The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. | Agiloft provides the ability to generate accurate and complete copies of records in both human readable and electronic form. Records may be printed both on paper and to a file; they also can be exported in PDF, Word, Excel, .CSV and TXT formats for inspection, review, and copying by the agency. |
| **(c)** Protection of records to enable their accurate and ready retrieval throughout the records retention period. | Automated system backups export records in a format that ensures full accuracy and allows them to be retrieved throughout the record retention period. |
| **(d)** Limiting system access to authorized individuals. | Agiloft access controls include login/password controls and security group permissions that limit access to authorized individuals. In addition, access may be limited based upon the user's IP address. |

| Sec. 11.10 Controls for closed systems. | Agiloft Compliance |
|---|---|
| **(e)** Use of secure, computer-generated, timestamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | Agiloft provides secure, computer-generated, timestamped audit records that independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Not only does History capture all changes made by users, but the entire record as it existed at any time in the past may be retrieved. Security groups can be configured to prevent the deletion of records and if a record is allowed to be deleted, Agiloft Activity Logs capture which user deleted it, the date/time that it occurred and the IP address from which they accessed the system. The retention period for audit logs may be configured by the administrator for periods up to 1,000 years and are available for agency review and copying. |
| **(f)** Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | The configurable workflow and validation rules allow administrators to set up a workflow that is appropriate for the process being managed and enforces the permitted sequencing of steps or events. |
| **(g)** Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | Agiloft uses a set of rules based on security group settings that uniquely identifies the user from their username and password combination. The internal security settings in these tools determine the access and privileges of the logged in user and ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. |
| **(h)** Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | Agiloft includes API's to integrate with hardware devices that can provide terminal checks to determine the validity of the source of data or operation instruction. As a software product, it does not include the use of specific hardware. |
| **(i)** Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. | Access is controlled via security groups to those individuals deemed appropriate and can be configured to prevent the group assignments to individuals whose user records do not certify them as having the education, training and experience to warrant their inclusion in such groups. The customer is ultimately responsible for providing the necessary education and training. |

| Sec. 11.10 Controls for closed systems. | Agiloft Compliance |
|---|---|
| **(j)** The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. | The customer is responsible for adhering to this requirement. |
| **(k)** Use of appropriate controls over systems documentation including: | |
| **(1)** Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. | The system includes generic online help, tutorials and documentation on system capabilities.<br>Access control and distribution of attached files containing documentation for system operation and management are managed by Agiloft Rules. |
| **(2)** Revision and change control procedures to maintain an audit trail that documents timesequenced development and modification of systems documentation. | Revision and change control procedures for system specific documentation are supported through Workflow Actions and Guards while History and Audit logs document the development and modification of system documentation. |

| Sec. 11.30 Controls for open systems. | Agiloft Compliance |
|---|---|
| Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | Agiloft can be used as an open system or a closed system depending on the access to the server via an IP address and port. Through the use of the username and password combination and internal security groups, the administrator has the ability to secure the system as required for compliance. |

| Sec. 11.50 Signature manifestations. | Agiloft Compliance |
|---|---|
| **(a)** Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: | Agiloft supports these requirements as detailed below: |
| **(1)** The printed name of the signer; | The name of the signer is displayed. |
| **(2)** The date and time when the signature was executed; and | A date and timestamp are clearly displayed and maintained by History |
| **(3)** The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | The meaning associated with each signature is captured in the associated field description. |
| **(b)** The items identified in paragraphs (a)(1), (a) (2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout). | Items (a)1,2,3 are subject to the same controls as electronic records and are included in any human readable form of the electronic record as controlled by access permission. |

| Sec. 11.70 Signature/record linking. | Agiloft Compliance |
|---|---|
| Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. | Electronic signatures are directly linked to their electronic records through DocuSign.<br>Such signatures cannot be excised, copied or otherwise transferred. Further, the history of every record modification performed in Agiloft is not modifiable and contains the details of the action taken as well as a timestamp and the user who performed the action. |

## Subpart C – Electronic Signatures

| Sec. 11.100 General requirements. | Agiloft Compliance |
|---|---|
| **(a)** Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | The unique username/password combination and two factor authentication required by DocuSign ensure the signature is unique to each individual and cannot be reused. Further, all records created by a user are permanently linked to the creator's unique username, and only the logged in user's name may be placed into a signature field by that user. |

| Sec. 11.100 General requirements. | Agiloft Compliance |
|---|---|
| (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. | The administrator is responsible for verifying that each user entered into the system is properly identified before entering a unique username and password combination for said user and sanctioning their use of an electronic signature.<br>Administrators can set strong passwords rules that are applied universally, including the ability to enforce a minimum password length, both alphabetic and numeric values in a password, mixed case letters in a password and dictionary words usages. The system controls incorrect password usages, locks the user's account for 5 minutes after a configurable number of invalid entries and invalidates passwords after a configurable number of invalid entries. Passwords can optionally expire in "x" days. **LDAP can be used instead of these features to centrally manage users.**<br>**All records created by a user are permanently linked to the creator's unique username.**<br>**The organization is responsible for sanctioning an individual's access to the system.** |
| (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. | This requirement is supported by the Agiloft / DocuSign integration and the customer is responsible for implementing it. |
| (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. | The customer is responsible for this requirement. |
| (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. | The customer is responsible for this requirement. |

| Sec. 11.200 Electronic signature components and controls. | Agiloft Compliance |
|---|---|
| (a) Electronic signatures that are not based upon biometrics shall: | Agiloft satisfies these requirements as detailed below: |
| (1) Employ at least two distinct identification components such as an identification code and password. | The Agiloft / DocuSign integration fully supports two factor authentication. |
| (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. | This is supported by Agiloft / DocuSign integration, the specific configuration is the responsibility of the customer administrator.<br>The system may further be configured to require that the user enter an additional identification code with each signing. |
| (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. | This is supported by Agiloft / DocuSign integration, the specific configuration is the responsibility of the customer administrator. |
| (2) Be used only by their genuine owners; and | The customer is responsible for this requirement. |
| (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | This is supported by Agiloft / DocuSign integration, the specific configuration and with two factor authentication enabled, attempted use of an individual's electronic signature by anyone other than its genuine owner would require the collaboration of the system administrator as well as the malicious individual. |
| (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | Agiloft includes API's to integrate with biometric hardware devices. As a software product, it does not include the use of specific hardware. |

| Sec. 11.300 Controls for identification codes/passwords. | Agiloft Compliance |
|---|---|
| Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: | Acknowledged |

| Sec. 11.300 Controls for identification codes/passwords. | Agiloft Compliance |
|---|---|
| **(a)** Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. | Agiloft uses a username and password to uniquely identify the person logged into the system and enforces that no two individuals can have the same username and password |
| **(b)** Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | Administrators can set strong password rules, including timed expiration rules, that are applied universally. LDAP can also be used to centrally manage users. |
| **(c)** Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | The customer is responsible for this requirement. |
| **(d)** Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | Agiloft supports the restriction of system access based upon IP address and as an additional safeguard may be configured to trigger immediate notifications to the system security unit and organizational management if an unusual pattern of activity is detected. |
| **(e)** Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. | The customer is responsible for this requirement. |

Authority: 21 U.S.C. 321-393; 42 U.S.C. 262.
Source: 62 FR 13464, Mar. 20, 1997, unless otherwise noted.

## ABOUT AGILOFT

Over 3 million users at organizations ranging from small enterprises to U.S Government agencies and Fortune 100 companies depend on Agiloft's top rated product suites for Contract Management, Service Desk, Custom Workflow, and more. Agiloft specializes in automating processes that are too complex for competing vendors. Our best practice templates and agile technology ensure rapid deployment and a fully extensible system. For more information, visit https://www.agiloft.com.