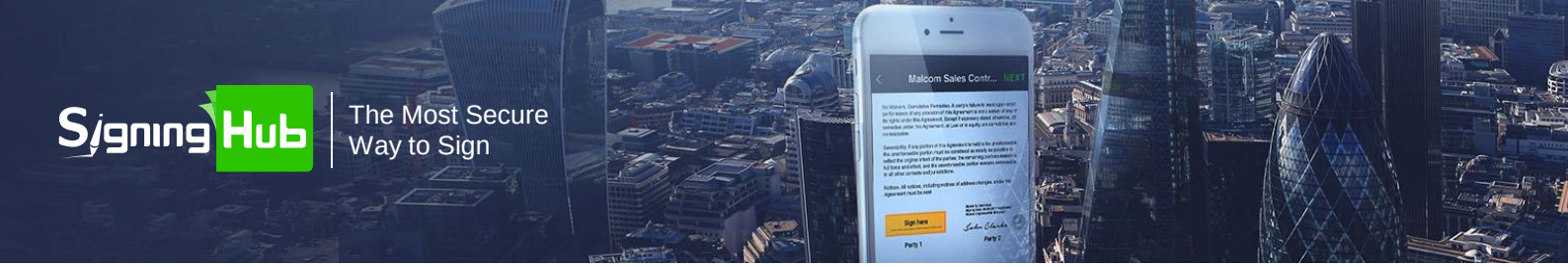

SigningHub and FDA 21 CFR 11 Compliance

SigningHub complies with the requirements of 21 CFR 11 as described below. Only the relevant sections from the FDA 21 CFR Part 11 requirements are repeated here.

ASC: Ascertia's comments on its compliance are shown in this way below each requirement.

21 CFR 11 Sec. 11.1 Scope.

STATEMENT

(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 accepted by regulation(s) effective on or after August 20, 1997.

(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.

(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.

21 CFR 11 Sec. 11.2 Implementation.

STATEMENT

(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.

STATEMENT

(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:

(1) The requirements of this part are met; and

(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, and 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.

21 CFR 11 Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(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.

(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.

ASC: SigningHub provides secure, well controlled and audited document management.

(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.

ASC: SigningHub offers secure, audited cryptographic trust services to meet these needs.

(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.

(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.

ASC: SigningHub provides document workflow and digital signature approval using both a digital signature and an electronic signature image to satisfy both the cryptographic integrity requirements and the human factors requirements for a visible signature. This can be used for both closed and open systems.

21 CFR 11 Subpart B--Electronic Records

21 CFR 11 Sec. 11.10 Controls for closed systems.

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:

ASC: When dealing with electronic documents SigningHub meets these requirements using the latest applicable industry standards. Authenticity and integrity are provided by using strong digital signatures and the system uses AES-256 bit encryption for all documents within the system at an application level so that data is protected even across systems and networks (for example to networked database systems). The Initial document upload is protected using an AES encrypted TLS/SSL session.

When dealing with other records such as XML data and other file types ADSS Server can be used to sign, verify and long-term archive the data.

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

ASC: SigningHub processes PDF documents and enables their digital signature approval. This is done using the following process steps:

1) The document is shown to the intended authorised user in a flattened image mode so no dynamic or potentially malicious code running within the document can change its content;
2) The user can see the document they are being asked to sign, they can fill in any form fields and apply initials that may be required before the signing operation;

3) When the user wishes to sign, they are re-authenticated and the user's unique digital signature is created and embedded in the document together with details of their name, the date and time of signing and the reason for signing;
4) The signature created is a long-term signature with an embedded timestamp and validation data and all these details can be verified immediately by the user or other recipients.

The signature meets ISO 32000 PDF standards and ETSI PAdES signature standards.

(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.

ASC: Any document signed with SigningHub can be viewed and the signature verified using the ubiquitous Adobe Reader products, and other standards compliant PDF viewer technology. If print permissions have been granted by the owner the document can also be printed out.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

ASC: SigningHub uses the latest standards recommended by the US National Institute of Standards and Technology (NIST) namely SHA-256 hashing and RSA 2048 bit digital signatures. Depending on system configuration the digital signatures produced can be valid for 20+ years. Furthermore SigningHub can convert documents to the long-term PDF Archive format referred to as PDF/A.

(d) Limiting system access to authorized individuals.

ASC: SigningHub provide effective access controls and provides enhanced security including password policy control. For higher security other authentication mechanisms such as SMS OTP, Client TLS/SSL authentication and even cryptographic mobile phone authentication can be used. SigningHub administrators are strongly authenticated using a client TLS/SSL certificate as part of a client/server mutually authenticated session.

(e) Use of secure, computer-generated, time-stamped 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.

ASC: SigningHub produces long-term digital signatures that include a digitally signed and trusted RFC 3161 timestamp from a Time Stamp Authority. SigningHub also records an activity log for all interactions with the document. The activity log contains a traditional date/time stamp against each log record.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

ASC: A core function of SigningHub is to enforce the defined workflow and allow or deny user access and actions as appropriate on documents that they need to review and approve.

(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.

ASC: A core function of SigningHub is to enforce user authentication, data access permissions including date embargos, signing actions (who, where, how and in which order) and thus maintain trust and data integrity.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

ASC: SigningHub authenticates all users or systems that upload documents to the system. A What You See Is What You Sign (WYSIWYS) approach is implemented so that users can always verify each document is what they expect before they create their unique digital signature.

(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.

ASC: SigningHub has an intuitive interface and offers optional tooltips and navigation guidance features to aid new users as they use the system. Any form fields that must be filled in can have this action enforced by the system so that the user cannot sign the document until their mandatory action fields are completed. On-line documentation and videos are available.

(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.

ASC: This requirement is out of scope for SigningHub.

(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.

ASC: This requirement is out of scope for SigningHub.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

ASC: SigningHub can be used as part of such an audit trail to record document change approvals.

21 CFR 11 Sec. 11.30 Controls for open systems.

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.

ASC: SigningHub meets these requirements using the latest applicable industry standards. Authenticity and integrity are provided by using strong digital signatures and the system uses AES-256 bit encryption for all documents within the system at an application level so that data is protected even across systems and networks (for example to networked database systems). When documents are uploaded they are protected using a secure TLS/SSL session.

21 CFR 11 Sec. 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

ASC: SigningHub complies as mentioned below.

(1) The printed name of the signer;

ASC: SigningHub enforces this using the PDF signature appearance controls. The signers name is also available from within the digital signature itself e.g. when verified using Adobe Reader.

(2) The date and time when the signature was executed; and

ASC: SigningHub enforces this using signature appearance controls and also from information contained within the digital signature. Long-term PAdES signatures are created which embed a timestamp from a trusted timestamp authority.

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

ASC: The meaning and reason for signing is incorporated into the digital signature, it can also be shown in the signature appearance stamped on the document. The signer can be notified in advance of the significance of applying a digital signature through a configurable legal notice that must be accepted before applying a digital signature.

(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).

ASC: SigningHub enforces this using digital signature controls and the visible signature within the PDF is a part of the document and thus is also printable.

21 CFR 11 Sec. 11.70 Signature/record linking.

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.

ASC: ISO 32000 defines the way in which digital signatures are applied to PDF documents. Any change to the document protected by a digital signature breaks the signature in way that is very obviously shown to any person reading the document using products such as Adobe Reader.

21 CFR 11 Subpart C--Electronic Signatures

21 CFR 11 Sec. 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

ASC: SigningHub always assigns each user a unique key and certificate. It can also use individual high-trust digital keys and certificates issued by internal or external CAs and held locally by the user on secure smartcards/USB tokens or other Secure Signature Creation Devices (SSCDs).

(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.

ASC: SigningHub provides mechanisms to control user registration and thus allows the organisation to enforce its Know Your Customer (KYC) rules on system access and use.

(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.

ASC: The notification process itself is out of scope for SigningHub. As explained before the user can be warned of the legal significance of their actions by a legal notice shown

immediately prior to them creating a digital signature on the document if configured by the system administrator.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.

ASC: The notification process itself is out of scope for SigningHub.

(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.

ASC: This requirement is out of scope for SigningHub.

21 CFR 11 Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

ASC: SigningHub enforces this using following methods:

a) username and password, or
b) username, password and SMS OTP or
c) using a local Client SSL certificate that is authenticated as part of a high trust client-server mutually authenticated session, or
d) using smartcard/USB token which holds the signing key and is protected with a PIN
e) using a mobile phone which holds the signing key (in software or secure hardware) and is protected with PIN/password

(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.

ASC: SigningHub enforces a signing password to be used, and optionally an SMS OTP authentication code, for every signing action. Where smartcards or other local signing keys are used their PIN/Password security control is managed by the secure device.

(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.

ASC: SigningHub complies and requires the user to login to the system once again.

(2) Be used only by their genuine owners; and

ASC: SigningHub enforces user authentication before allowing access to the signing key. Multiple authentication options are available as explained above offering advanced levels of security.

(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.

ASC: SigningHub enforces strong user authentication and prevents this scenario even if multiple individuals are involved. For highest level of security we recommend locally-held signing keys so that only the signer has access to their keys (and these are PIN/password protected to prevent use when lost/stolen).

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

ASC: Full biometric signatures are not used by SigningHub. SigningHub does support hand-written signatures using either mouse, tablet stylus or a dedicated hardware signature device, but nevertheless these hand-written signatures are only used as images to aid acceptance from user perspective rather than to add biometric based security.

21 CFR 11 Sec. 11.300 Controls for identification codes/passwords.

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:

(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.

ASC: SigningHub enforces this.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

ASC: SigningHub enforces strong password policies and prefers this approach since enforcing regular password changes just means users write down their latest password - which is very weak. For even higher levels of security, SMS OTP can be used OR client-server SSL OR smartcard/USB devices OR mobile phone authentication/signing can be used.

(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.

ASC: SigningHub strictly controls the central keys and certificates it provides for users and so these cannot be lost. Any user account can be suspended as may be required. The control of externally managed local keys and certificates is out of scope for SigningHub and must be covered by other procedures applicable to the issuer CA.

(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.

ASC: SigningHub uses strong TLS/SSL to protect transactional data and to protect identification codes. A strong system of controls exists to prevent brute attacks on the system and optional password resets require addition authentication information to be entered.

(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.

ASC: SigningHub strictly controls the central keys and certificates it provides for users and so these cannot be lost. The control of externally managed local keys and certificates is out of scope for SigningHub and must be covered by other procedures applicable to the issuer CA.