

CastorSMS 2022.x.x

21 CFR Part 11 Assessment of Compliance

Document Version: 1.0

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

I. Subpart A - General Provisions

The purpose of this document is to describe CastorSMS compliance with the Food and Drug Administration's [TITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES, PART 11, ELECTRONIC RECORDS; ELECTRONIC SIGNATURES](#)

This document applies to CastorSMS 2022.x.x as internally developed and tested. CastorSMS has been designed and developed to be in compliance with 21 CFR Part 11, electronics records, electronic signatures and predicate rules when implemented and controlled effectively by the System User. Castor achieves compliance through a combination of risk assessment, SOP adherence, and by establishing a structured validated system. It is however the System User's responsibility to ensure that the software, as provided, is deployed and used in a manner that is compliant with 21 CFR Part 11. The stem includes features such as Security controls through different access permissions, Audit Trails, Electronic Signatures with integrity checks.

Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

System Name:	CastorSMS
System Version:	2022.x.x
System Description:	Castor is a cloud-based Study Management System (SMS) solution, allowing users to manage and track core information, documents and workflows during their study life cycles in one platform.

Definitions

Electronic Record – is 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 (refer to 21 CFR Part 11.3(b)(6)). Only records required by an agency regulation (FDA; Food, Drug & Cosmetic Act; or Public Health Services Act) to be maintained for inspection or to be submitted to an agency are considered within the scope of the 21 CFR 11 regulation. Note: a record is not considered to be “created” until it is committed to durable media.

Electronic Signature – is a digital representation 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 (refer to 21 CFR Part 11.3(b)(7)). For a signature to be considered an electronic signature under 21 CFR Part 11, it must be executed as the conscious action of the owner with a specific meaning (e.g., approval, release, review).

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

Computer System – is defined as a configuration of hardware components and associated software designed and assembled to perform a specific function or group of functions. Included in this definition are laboratory instruments, control systems, and computer systems, including hardware, software, peripheral devices, personnel, and documentation; e.g., manuals and Standard Operating Procedures. Third-party application software as well as internally developed application software is also included in this definition.

Regulation Reference – Reference to the specific paragraph in the 21 CFR Part 11 regulations.

System Supplier - Castor system being assessed

System User- Castor’s client, sponsor or CRO using the system being assessed.

II. Subpart B - Electronic Records

1.1 §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:

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

System Supplier	System User
Castor validates each release per internal SOPs. The System was developed using industry standard development tools and methodologies and was conforming to GxP requirements.	Users must assure themselves that System Supplier has validated system based on requirements and guidelines when developing and testing the System.

§11.10 (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.

System Supplier	System User
The System supports the ability to electronically display and print in human readable form most of the data contained within the system.	Responsible for providing copies of records for inspection by the agency.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

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

System Supplier	System User
<p>For Castor hosted solutions, all data is backed up routinely per established SOPs. Data backups are performed twice per day. The restore process is tested every 3 months. Castor also follows standards for record retention periods.</p>	<p>Client is responsible for maintaining all study related data and following their own retention policies.</p>

§11.10 (d) Limiting system access to authorized individuals.

System Supplier	System User
<p>Only authorized individuals are given access to their specific installation of Castor SMS.</p> <p>Castor SMS employs role-based user access based on a user's responsibilities within an institute.</p> <p>The System includes a login mechanism that requires each user to log in with a unique username and password to gain access to the system. Functions such as password requirements are supported by the System.</p> <p>The System servers are housed in a secure, access controlled environment. Only authorized personnel have access to the servers. Castor has SOPs on how to assign system access to authorized personnel.</p>	<p>Castor SMS employs role-based user access based on a user's responsibilities within an institute.</p> <p>User is responsible for defining users and roles in the system. Should assign permissions based on role for access to different information within the system.</p>

§11.10 (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.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

System Supplier	System User
System has full audit trail. All information including date, time, user, old value and new value is captured in the audit trail. The audit trail is retrievable throughout the record's retention period and is available to the agency for review, inspection and copy.	Responsible for ensuring the vendor maintains the data and associated audit trails retained and available.

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

System Supplier	System User
The System has been designed to allow the System User to configure workflows that guide the end user through the proper sequence of events.	Responsible for configuring the System appropriately for their intended use.

§11.10 (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.

System Supplier	System User
Only authorized individuals can access and use the system by using email and password . Castor SMS has been designed to require username and password to gain access. The application uses a role based security model to restrict data access only to authorized users.	Responsible for configuring the System appropriately.

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

System Supplier	System User
Castor SMS does not use any device checks.	n.a.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

§11.10 (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.

System Supplier	System User
<p>Castor maintains CVs and JDs for staff that develop or maintain the System. They are hired based on education, training and/or experience, and properly trained according to Castor Policies and Procedures. Training records are maintained as per SOP.</p>	<p>It is the responsibility of the company deploying Castor SMS to ensure that their employees developing, maintaining/administering and using the system have the appropriate training, education and experience.</p>

§11.10 (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.

System Supplier	System User
<p>Castor requires users to accept Terms of Use when setting up a new user account for Castor SMS.</p>	<p>Responsible for ensuring appropriate policies are in place and that compliance with those policies are monitored.</p>

§11.10 (k) Use of appropriate controls over systems documentation including:

§11.10 (k) (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

System Supplier	System User
<p>System documentation can only be accessed by authorized individuals.</p> <p>Castor provides an online resource library and Castor Academy for users to have access to Manuals and User Guides with step-by-step instructions on how to get the most out of Castor systems.</p>	<p>Sites are responsible for the creation and maintenance of their own documentation that supports the operation and maintenance of the System.</p>

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

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

System Supplier	System User
All documentation is electronically version controlled and any alteration is handled via change controls.	Responsible for the change control documents supporting their production environment.

1.2 §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.

Supplier	System User
Only authorized individuals can access and use the system. Castor SMS has been designed to require username and password to gain access. The application uses a role based security model to restrict data access only to authorized users.	Responsible for configuring the System appropriately.

1.3 §11.50 Signature Manifestation

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

§11.50 (a) (1) The printed name of the signer; (2) The date and time when the signature was executed; (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

System Supplier	System User
Castor SMS clearly indicates the name of the signer, local date/time of the signature and the meaning associated with the signature for each electronically signed approval request.	Responsible for configuring the System appropriately.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

An approval request can only be signed by users who have the associated approval request role, or by admin users.	
---	--

§11.50 (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).

System Supplier	System User
This information is contained in the audit trail which is displayed in human readable format.	Responsible for configuring the System appropriately.

1.4 §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.

System Supplier	System User
All data is digitally signed using user's credentials.	Responsible for configuring the System appropriately.

2 Subpart C - Electronic Signatures

2.1 §11.100 General requirements

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

System Supplier	System User
Electronic signatures within Castor SMS are uniquely attributable to a single system user based on an individual's unique username and password.	Responsible for configuring the System appropriately and enforcing appropriate policies to prevent reusing or reassign a user's ID.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

§11.100 (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.

System Supplier	System User
Not applicable. System User's responsibility.	System User's responsibility to verify.

§11.100 (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.

§11.100 (c) (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.

System Supplier	System User
Not applicable. Castor sent letter regarding electronic systems used internally. This is the System User's responsibility.	Castor is not responsible for documenting the identity of system users. Responsibility for this task falls on the company deploying Castor SMS.

§11.100 (c) (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.

System Supplier	System User
Not applicable. Castor is not responsible for this task. This responsibility falls on the company deploying Castor SMS.	Castor is not responsible for this task. This responsibility falls on the company deploying Castor SMS.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

2.2 §11.200 Electronic signature components and controls

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

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

System Supplier	System User
When a user signs an approval request for the first time in a session after the login, the user is prompted to enter their "signing credentials" consisting of a username and password combination.	Responsible for configuring the System appropriately.

§11.200 (a) (1) (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 execute at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

System Supplier	System User
Castor SMS requires two distinct identification components (User ID and password) for all signings.	Responsible for configuring the System appropriately.

§11.200 (a) (1) (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.

System Supplier	System User
Castor SMS requires two distinct identification components (User ID and password) for electronic signatures not performed in the same system session.	Responsible for configuring the System appropriately.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

§11.200 (a) (2) Be used only by their genuine owners.

System Supplier	System User
This is covered in the Terms of Use agreed to by a user when initializing their Castor SMS user account.	Responsible for configuring the System appropriately and adopting and enforcing appropriate policies e.g. no username/password sharing. This is covered in the Terms of Use agreed to by a user when initializing their Castor SMS user account.

§11.200 (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.

System Supplier	System User
Use of an individual's electronic signature would require collaboration of two or more individuals. Either the user would have to provide the password to another user, or the system administrator would have to collaborate with the user.	Responsible for adopting and enforcing appropriate policies.

§11.200 3 (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

System Supplier	System User
N/A. Castor systems do not support the use of biometrics.	N/A

2.3 §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:

§11.300 (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.

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

System Supplier	System User
Each user has a unique user ID and password combination. Castor SMS is configured so that a strong password policy is enforced as well.	Responsible for configuring the System appropriately.

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

System Supplier	System User
Castor SMS does not support periodical password checks.	N/A

§11.300 (c) Following loss management procedures to electronically de-authorize 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.

System Supplier	System User
Castor is responsible for the password policy for clients (product users). In an event of a security breach or related problems, the Castor EDC and Castor SMS user passwords can be reset by a Platform Engineer with Production Server Access. This will force all users to reset their passwords upon login, by retrieving a password reset email.	Responsible for configuring the System appropriately and adopting and enforcing appropriate policies.

§11.300 (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.

System Supplier	System User
-----------------	-------------

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

<p>The System can be configured to automatically lockout a user ID after ten failed login attempts. The same functionality applies to electronic signature passwords.</p>	<p>Responsible for configuring the System appropriately and adopting and enforcing appropriate policies.</p>
---	--

§11.300 (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.

System Supplier	System User
<p>Tokens or cards used to generate identification codes or passwords are not utilized by Castor SMS.</p>	<p>Tokens or cards used to generate identification codes or passwords are not utilized by Castor SMS.</p>




Revision History

Document Version #	Description of Change	Author	Effective Date
1.0	Initial Release	Nienke Tjalma	14-MAR-2022

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.

Approval

The signatures below indicate approval of the content of this document.

Product Author	<p>DocuSigned by:</p> <p><i>Nienke Tjalma</i></p> <p> Signer Name: Nienke Tjalma Signing Reason: I am the author of this document Signing Time: 15-Mar-2022 3:33:28 PM CET 18AACAD9A8584EBB8548212CBA542587</p>
Name and Title	Nienke Tjalma, Product Owner
QA Approval	<p>DocuSigned by:</p> <p><i>Ben Driesen</i></p> <p> Signer Name: Ben Driesen Signing Reason: I approve this document Signing Time: 16-Mar-2022 8:59:17 AM CET 2EE2C77E7DD94FFC8D17A479F833A09D</p>
Name and Title	Ben Driesen , Manager of QA
Compliance Approval	<p>DocuSigned by:</p> <p><i>Fatma Elfaghi</i></p> <p> Signer Name: Fatma Elfaghi Signing Reason: I approve this document Signing Time: 16-Mar-2022 12:43:53 PM EDT 06D97C1F835640F7923003BDA1E2E782</p>
Name and Title	Fatma Elfaghi, Director of Quality and Compliance

This information is proprietary to Castor and should be treated as confidential material in accordance with existing confidentiality agreements. Unauthorized use of this data is strictly prohibited.