Castor eConsent 2022.x.x
21 CFR Part 11 Assessment of Compliance

Document Version: 1.0

I. Subpart A - General Provisions

The purpose of this document is to describe Castor eConsent 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 Castor eConsent version 2022.x.x as internally developed and tested. Castor eConsent 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:	Castor eConsent
System Version:	2022.x.x
System Description:	Castor electronic Informed Consent software (Castor eConsent) streamlines and automates participant recruitment, screening, and consenting processes. Designed for decentralized and hybrid research projects to deliver compliant, site-friendly, patient-centric experiences.
Comments:	The current version of Castor eConsent was evaluated from the URL: us.castorconsent.com / eu.castorconsent.com

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).
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. Qualification and requalification audits are available upon request based on internal procedures by contacting the Compliance department.

§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 all data contained within the system. Consent forms (signed and unsigned) can be exported/printed into a human readable PDF format.	Responsible for providing copies of records for inspection by the agency.

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

System Supplier	System User
For Castor hosted solutions, all data is backed up routinely per established SOPs. Data backups are performed automatically throughout the day. Castor also follows standards for record retention periods.	Client is responsible for maintaining all study related data and following their own retention policies.

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

System Supplier	System User
Only authorized individuals are given access to specific clinical studies within Castor eConsent. Castor eConsent can integrate with external identity providers allowing users to access the system being authenticated with external set of credentials (aka: Single Sign-On.) Castor eConsent employs role-based user access based on a user's responsibilities within a specific clinical study. 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. 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.	Castor eConsent employs role-based user access based on a user's responsibilities within a specific clinical study. User is responsible for defining users and assigning the roles in the system. Should assign permissions based on role for access to different information within the system.

§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.

System Supplier	System User
System has a full audit trail. All information including, action, 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 enforce permitted sequencing of steps. For example the order of users that can sign a consent form and the statuses of consent forms.	Responsible for configuring the System appropriately.

§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. Castor eConsent 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. In addition, eConsent can also integrate with external identity providers to allow for Single Sign-On. In this case, the third party system is responsible to provide proper control for authentication. It includes actions such as logging in and signing of ICF.	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 verifies source of access by the data stored after login in the API response (eg. login attempts, date & time, timezone for the user who is logged in). In addition, to confirm the integrity of the data that is being entered into the consent forms, any device/system used to enter data into our system	Responsible for configuring the System appropriately.

(outside of keyboard and mouse being tested implicitly throughout the validation) such as a bar code reader, data integration would include some test (within the system directly leveraging the edit-checks) or outside the system through specific test steps (in API connection, error code returns success or failure for the entry).	

§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
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.	It is the responsibility of the company deploying Castor eConsent for their clinical trial (e.g. Sponsor, CRO) to ensure that their employees developing, maintaining/administering and using the system have the appropriate training, education and experience.

§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
Castor requires users to read Terms of Use when setting up a new user account for Castor eConsent. The Terms of Use are not applicable for users that log in via SSO.	Responsible for ensuring appropriate policies are in place and that compliance with those policies are monitored.

§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

System documentation can only be accessed by authorized individuals. Castor provides an online resource library with step-by-step instructions on how to get the most out of Castor systems.	Sponsors are responsible for the creation and maintenance of their own documentation that supports the operation and maintenance of the System.

§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.

System Supplier	System User
Only authorized individuals can access and use the system. Castor eConsent 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. The system has been designed to be able to use industry standard TLS encryption for secure communications across the network. Data integrity: Traceability: - Depending on the context, changes made to the data can be rolled back or additional verification of the change is requested from the user. - User accounts are always traceable to a person. In combination with the audit log, it is possible to trace back which person made a change. - The audit log allows to trace back when data was changed. Backup: - Automated backups are executed automatically. See §11.10 (c).. Application controls: - Where possible, the interface only allows valid inputs from being chosen (white-listing). When not possible, the interface checks the user input after it has been given and provides validation messages. - The API provides, at least, the same validation as the interface to ensure data validity. - Database integrity checks automatically validate the integrity of data relations. Non-repudiation of data: - The audit log enables us to determine who changed changed what, when. - Audit logs are immutable. Non-repudiation of application: - Users are allowed to make changes to application data based on their roles. - Roles and their corresponding rights are constructed to support the principles of “segregation of duties” and “least privilege”. - Access to fully privileged “root” accounts is strictly regulated.	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 eConsent clearly indicates the name of the signer and local date/time of the signature for each electronically assigned record. The meaning of the signature (Signature Statement in eConsent) can be configured per consent form. The information stored for each eSignature contains a reference to username (email address).	Responsible for configuring the System appropriately. Castor does not create the content of the consent form, it is the sponsor that creates the content. It is the responsibility of the sponsor to add the meaning of signature.

§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. The audit trail contains information including, date, time, user, old value and new value. The audit trail can be exported by Castor upon request.	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 (username and password). Electronic signatures within Castor eConsent are uniquely attributable to a single system user based on an individual's unique username and password.	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 eConsent are uniquely attributable to a single system user based on an individual's unique username (email address) and password.	Responsible for configuring the System appropriately and enforcing appropriate policies to prevent reusing or reassign a user's ID.

§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 eConsent for their clinical trial (e.g. Sponsor, CRO).

§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 eConsent for their clinical trial (e.g. Sponsor, CRO).	Castor is not responsible for this task. This responsibility falls on the company deploying Castor eConsent for their clinical trial (e.g. Sponsor, CRO).

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 any consent form, the user is prompted to enter their "signing credentials" consisting of a username (email address) 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 eConsent requires two distinct identification components (username and password) during each time the user signs.	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 eConsent always requires two distinct identification components (username and password) for electronic signatures.	Responsible for configuring the System appropriately.

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

System Supplier	System User
This is covered in the Terms of Use that has to be read by a user when initializing their Castor eConsent user account. However, with SSO, this is not applicable because the user is NOT ticking the "Terms of Use" checkbox.	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 eConsent 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.

System Supplier	System User
Each user has a unique username (email address) and password combination. eConsent is configured so that a strong password policy is enforced as well. eConsent does support SSO, password policy is then configured by the external identity provider.	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
eConsent does not support the periodic check, recall or revise of passwords. eConsent does support SSO, password policy is then configured by the external identity provider.	Responsible for configuring the System appropriately and adopting and enforcing appropriate policies.

§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 the event of a security breach or related problems, the Castor eConsent user passwords can be reset by Castor staff. Users have individual accounts and strong passwords are required. Users are locked out of their account after 10 failed login attempts. The user stays locked out for 12 hours. Sessions automatically time out after 30 minutes of inactivity.	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
The System is configured to automatically lockout a user ID after a pre-determined number of failed login attempts (10 times). eConsent can integrate with external identity providers to allow for Single Sign-On.	Configuring the System to force appropriate policies is not possible.

§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
Tokens or cards used to generate identification codes or passwords are not utilized by Castor eConsent.	Tokens or cards used to generate identification codes or passwords are not utilized by Castor eConsent.

Revision History

Document Version #	Description of Change	Author	Effective Date
1.0	Initial Release	Frouke Karel	15-MAR-2022

Approval

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

Product Author	DocuSigned by: Frouke Karel Signer Name: Frouke Karel Signing Reason: I am the author of this document Signing Time: 24-mrt-2022 | 3:36:58 PM CET FDFC361715F14E72B35E3ABF0BF2AC80
Name and Title	Frouke Karel, Product Owner
QA Approval	DocuSigned by: Ben Driesen Signer Name: Ben Driesen Signing Reason: I approve this document Signing Time: 28-Mar-2022 | 9:58:11 AM CEST 2EE2C77E7DD94FFC8D17A479F833A09D
Name and Title	Ben Driesen, Manager of QA
Compliance Approval	DocuSigned by: Fatma Elfaghi Signer Name: Fatma Elfaghi Signing Reason: I approve this document Signing Time: 29-Mar-2022 | 11:17:45 AM EDT 06D97C1F835640F7923003BDA1E2E782
Name and Title	Fatma Elfaghi, Director of Quality and Compliance