Castor Assessment of GDPR and HIPAA Compliance

GDPR Compliance	Relevant articles of the GDPR	Implementation
Principles relating to processing of personal data. **Employee awareness training**	**Article 5**	Personal data of Castor Employees is collected solely to support their work at Castor. For Customers, personal data is collected solely to support and improve their interactions with Castor. This primarily requires each contact's full name, username, title/role, email address, phone number and job responsibilities. For Patients, the entry and use of personal data is the responsibility of the Customer. Castor provides secure hosting of the applications and corresponding databases. Only limited personnel within Castor have access to production databases based on their role. Authorizations are granted on the 'need to know' and 'least privilege' principles. These access restrictions are described in SOPs. (See Castor's Security Statement.) All employees are aware of their commitment to protect patient information and are properly trained in Data Security and Data Privacy, including GDPR, and HIPAA. Castor ensures that data is processed according to the following principles: - Lawfulness , fairness and transparency; - Collected for specific, explicit and legitimate purposes; - Data minimisation; - Accuracy; - Integrity and confidentiality.
Lawfulness of processing	**Article 6**	Castor performs no processing of personal data other than is necessary to manage its Employees, support its Customers, respond to prospective Customers and fulfill its obligations to manage clinical trial data based on contractual requirements with Customers.
Conditions applicable to child's consent	**Article 8**	Castor assumes that, for Patients in pediatric trials, informed consent is signed by the child's authorized representative. Therefore no additional provisions are required for a child's consent. Ultimately, this is the responsibility of the Customer.

Version 2.0

Processing of special categories of personal data	**Article 9**	No such personal data is collected directly from Customers by Castor. For Patients, where medical, genetic, or biometric data is processed, Castor acts strictly as a Data Processor and supports the legal architecture determined by the Customer (Data Controller). While Customers may utilize explicit informed consent, Castor's platform is fully capable of supporting alternative processing conditions under Article 6(1)(c)/(f) and Article 9(2)(j) of the GDPR (processing for scientific research purposes), in alignment with EDPB Opinion 3/2019 on clinical trials. Data is protected using state-of-the-art technical and organizational security measures.
Privacy Statement	**Article 5, 12, 13, 14, 15,**	By visiting Castor's websites and by using its services, website visitors and Customers are trusting Castor with their personal data. In the privacy and cookie statement Castor explains which data it collects and for which purposes. See Castor's Privacy and Cookie Statement.
Data Portability	**Article 20**	Participants of investigational studies must request data through Investigator, Sponsor, or CRO. The Data Controller will contact Castor with any requests. Castor has a documented procedure in place to carefully handle these specific requests. Our "Data Subject Request Procedure" describes this process. It can be reviewed during audits.
Data Retention Policy	**Article 5, 13, 16, 17, 21 and 30**	Patient data is retained in Castor's databases for up to 25 years after study completion, explicitly mapping to the statutory compliance requirements of Article 58 of the EU Clinical Trials Regulation (CTR - Regulation No 536/2014), or deleted sooner upon the direct instruction and contract termination by the Customer. Castor's "Document management and data retention policy" can be reviewed during audits.
Security of processing	**Article 5, 18, 32**	Integrity and honesty are the key attributes of everything we do at Castor. We are committed to protecting our customers' data above all else. Castor is secured according to the most recent standards in order to protect your data in the best possible way. See Castor's Security Statement.
Appointment of DPO	**Article 37-39**	Castor has appointed an internal DPO in order to comply with the obligations under the GDPR.
Data Subject Rights Policy	**Article 15-23**	Castor has a documented procedure in place to carefully handle these specific requests. Our "Data Subject Request Procedure" describes this process. It can be reviewed during audits.
Responsibility of the Controller	**Article 24, 28**	Castor is the controller of Employee data; and the processor of Patient data. Appropriate SOPs and security measures have been put in place to ensure correct organizational processes are followed when collecting and handling personal data. Security measures and the associated tools for managing security are outlined in more detail in Castor's "Information

		Security Policy", which can be accessed during audits. General Information disclosed in Castor's Security Statement.
Privacy by design and by default	**Article 25**	"Secure Development Procedure", "Validation Procedure" and "Security/Privacy by Design Checklist" describe how these measures are implemented. Authorizations to internal environments and systems are granted on the 'need to know' and 'least privilege' principles.
Data Processing Agreement (Castor customers) Engaging Sub Processors	**Article 28**	Castor's obligations towards its Customers are covered under the Master Service Agreement (MSA). Castor also maintains a Supplier procedure that includes the completion of a Data Processing Agreement (DPA).
Data Processing Agreement (Suppliers - Castor as Controller)	**Article 24 and 28**	Castor has a specific procedure in place to make sure products and services are purchased with suppliers who comply with Castor's selection criteria and are onboarded according to Castor requirements (including the correct documentation), both to make sure all purchased products and services comply with the quality and information security standards needed for Castor.All details are covered under DPA's.
Records of processing activities	**Article 30**	Documented in the "Castor GDPR - Processing Activity Register." In compliance with Article 30(2) GDPR, Castor maintains a comprehensive internal register of all categories of processing activities carried out as a Processor on behalf of its Customers. For Patient data, the Client, Sponsor or CRO maintains the primary Controller register under Article 30(1). Castor's Master Service Agreements (MSA) and DPA's clearly delineate the specific processing parameters, categories of data subjects, and approved sub-processors.
Data breach procedure	**Article 28, 33 and 34**	If a data breach poses a risk to an individual's rights and freedoms, Castor has a "Personal Data Breach management procedure" in place to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach. If Castor operates as a data processor it will notify every data breach to its Customer(s) within 48 hours.
Cooperation with the supervisory authority	**Article 31**	Castor has a detailed process for reporting incidents to the supervisory authority, "Data Breach Management Procedure", in addition to the process for supporting a regulatory inspection,"Regulatory Inspections and Client Audits Procedure".
Records of (possible) data breaches	**Article 33**	Castor has an overview of all (possible) security incidents and data breaches, managed through Jira QMS.

Data Privacy Impact Assessment	**Article 35**	A Data Protection Impact Assessment (DPIA) is a process that helps identify and minimize the data protection risks of a particular service or product. As Castor acts as a Data Processor, the legal obligation to conduct a formal Data Protection Impact Assessment (DPIA) resides with the Data Controller (the sponsor/CRO) under GDPR Article 35. However, as outlined in Castor's MSA, Castor actively assists Clients with this process. To fully support our Clients' DPIA requirements, we can share recent DPIA examples alongside this Assessment-of-GDPR-and-HIPAA-Compliance document. These documents fulfill all vendor-side privacy and risk assessment needs by detailing our data flows, organizational safeguards, and dual GDPR/HIPAA compliance.
Transfers subject to appropriate safeguards	**Article 46**	Standard Contractual Clauses (SCCs) for transfers of personal data outside the European Economic Area (EEA) or the UK are fully executed within Castor's standard DPA. In strict adherence to EDPB Recommendations 01/2020 (following the Schrems II ruling), Castor performs Transfer Impact Assessments (TIAs) where required and implements supplementary technical measures - including strong data pseudonymization and advanced end-to-end encryption standards - to guarantee an equivalent level of protection for international data flows.
Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.	**Article 89**	General information disclosed in Castor's Security Statement

Castor HIPAA Compliance

Castor ensure compliance with HIPAA requirements through:

- ✓ Periodic Awareness Training to all employees
- ✓ Establishment of data privacy and security policies and procedures, including Data Breach Policy and regular updates to policies and procedures to align with the latest HIPAA regulations and best practices
- ✓ Risk Analysis and Management to track access of PHI
- ✓ Administrative Safeguards: Security Management, Security Training, Information Access Management
- ✓ Technical safeguards to protect access to data, including access control, audits controls, data integrity, authentication and transmission security and continued monitoring of systems to detect and respond to security incidents promptly
- ✓ Data Integrity Controls and regular audits and validation checks to maintain integrity
- ✓ Periodic reviews and Internal Audits to evaluate the effectiveness of security measures and implementing corrective actions based on audit findings
- ✓ Designation of a dedicated HIPAA Privacy Official and Security Official to oversee compliance requirements
- ✓ Execution of mandatory Business Associate Agreements (BAAs) with all HIPAA-covered Customers and downstream sub-contractors handling PHI