DATA PROTECTION IMPACT ASSESSMENT

Context

This section gives you a clear view of the processing of personal data in question.

OVERVIEW

This part allows you to identify and present the object of the study.

What is the processing under consideration?

The EBVOLVE study is an observational, multicenter, multinational Post-Authorisation Safety Study (PASS).

This study is conducted solely for scientific research and public interest purposes to describe and characterize the safety and effectiveness profile of tabelecleucel in subjects with EBV+ PTLD following Hematopoietic Cell Transplantation (HCT) or Solid Organ Transplantation (SOT), in a real-world setting in Europe.

The study is mandated by the European Medicines Agency (EMA) and the study protocol was approved by the Pharmacovigilance Risk Assessment Committee (PRAC), the European Medicines Agency's (EMA) committee responsible for assessing and monitoring the safety of human medicines. During its review of the marketing authorisation application for tabelecleucel, the EMA requested additional data collection on safety and effectiveness of tabelecleucel, including long-term outcomes, particularly in paediatric (aged < 18 years) and elderly (aged ≥ 65 years) populations due to the limited evidence available. This PASS protocol addresses the limited evidence in these special populations (paediatric and elderly) and will characterise further the long-term safety and effectiveness of tabelecleucel in the overall EBV+ PTLD subject population in a real-world setting in compliance with European Health Authority guidelines for advanced therapy medicinal products.

What are the responsibilities linked to the processing?

Pierre Fabre Medicament (PFM) is the sponsor and data controller based in France
Other processors and controllers in the cell selection process and delivery include:

- Pierre Fabre's third-party vendors acting data processor:
  SalesForces as provider and hoster of the Go Cell Therapy Portal

- Oracle France SaS (and affiliates), Global CRO based in France, is commissioned by PFM for their full services to conduct the study (study documents, EDC set-up and management, start-up activities, data collection, data management, statistical analysis, clinical study report, Trial Master File through PFM system, archiving) and conduct site study activities in European countries. Oracle France SaS and its affiliates act as data processor.

Oracle is in charge of development of the electronic case report forms (eCRF) through the electronic data capture system, called Oracle® Life Sciences Clinical One Cloud Service (Clinical One). This system is developed and designed for online data entry, data management and data validation for clinical studies.

- Medical Sites (e.g. hospitals, clinics, etc.) based in Europe, that house medical data collected, personal medical/health records and other personal identifiable information, related to the subject, which shall be considered Independent Controllers. Principal investigators and the authorized site staff, employee of the Medical Sites, will be in charge to trigger the data importation from the Go Cell Therapy (GCT) Portal, to the eCRFs via Oracle ClinicalOne, and they will be in charge of data abstraction from subject medical record (primary data) and documentation of the eCRF via ClinicalOne. Depending on the EU countries regulation, medical sites are considered as data processor or joint controller.

Are there standards applicable to the processing?

The European regulation no 2016/679 as known as General Data Protection Regulation (GDPR) enforced since 25 May 2018.

Local Data Protection laws in each EU country involved in the study, when applicable

Italy specificity:

On April 23, 2024, the Italian Parliament approved an amendment to the Italian Privacy Code related to the Article 110 of the Italian Privacy Code about "medical, biomedical and epidemiological research". It repeals the obligation for Sponsors to consult the Italian Data Protection Authority (Garante) and obtain their approval before conducting research involving the health data processing for scientific purposes, and when it is impossible to obtain the consent of the patients, or informing the data subjects is "impossible" or involved "a disproportionate effort" or risked "preventing or seriously harming the achievement of the research objectives".

Despite this exemption, PFM put in place appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects before personal data processing:

- The Data Protection Impact Assessment that will be shared for the Garante for notification.
- The study will be reviewed and approved by the relevant Ethics Committee in Italy
- Living patients who have read the Privacy Information Notice and given their consent to the processing of personal data by signing the Informed Consent form, corresponding to the lawfulness.
- For lost-to-follow-up patients, the sites did reasonable efforts to seek their consent at their last known addresses. The site detailed it in their medical patient charts.
- For deceased patients and Lost-to-follow-up patients not reachable, since this would entail a disproportionate effort or the risk to jeopardize the purpose of the Study according to Article 14(5) and recital 62 of the GDPR, an information notice will be published on PFM website and on Site website, as well as posted in site waiting room, when it is possible, allowing the legal representative, guardians, lost to follow-up patients to have access to the Privacy Information Notice and exercise their rights.

GO Cell Therapy specificity

GO Cell Therapy (Salesforce portal)
ASIP Santé HDS
C5 ISAE 3000 (Revised)
FISC (Japan)
HiTrust
IRAP
ISO 27001,ISO 27017,ISO 27018
NEN 7510-1:2017
PCI-DSS
SOC 1 Type II (SSAE 18 Report)
SOC 2 Type II (Trust Principles Report)
TRUSTe Certified Privacy Seal
FedRAMP (NIST 800-53),
PrivacyMark from the JIPDEC

For more details, the following website may be consulted https://compliance.salesforce.com/

A Data Protection Impact Assessment related to GO Cell Therapy (Salesforce portal) was developed and detailed in Appendix 4

Context

This section gives you a clear view of the processing of personal data in question.

DATA, PROCESSES AND SUPPORTING ASSETS

This part allows you to define and describe the scope of the processing in detail.

What are the data processed?

Data types	Recipients
Identifiable information of contractors, agents, consultants such as CRO, managing and executing with EBVOLVE study (complete full name, contact details), including contracts (MSA/SOW), invoices, administrative documents which need to be kept after the end of the study in case of audit/ regulatory authority request.	PFM (Sponsor) Oracle France SAS (Global CRO)
Identifiable information of the Principal investigators and other Health Care professional (HCP) involved in the EBVOLVE study (surname, first name, title, professional e-mail, postal address and telephone number, Curriculum vitae, License number) Medical sites : bank account details	PFM (Sponsor) Oracle France SAS (Global CRO)

Data types	Recipients
Pseudonymized subject demographic data: Year of birth, age, gender at birth	PFM (Sponsor) Oracle France SAS (Global CRO)
Pseudonymized subject medical data: relevant disease history, Subject characteristics, EBV+ PTLD at diagnosis, History and type of transplantation, on-treatment alloreactive event reporting, Treatment for EBV+ PTLD, basic treatment outcome by treatment cycle, safety information.	PFM (Sponsor) Oracle France SAS (Global CRO)

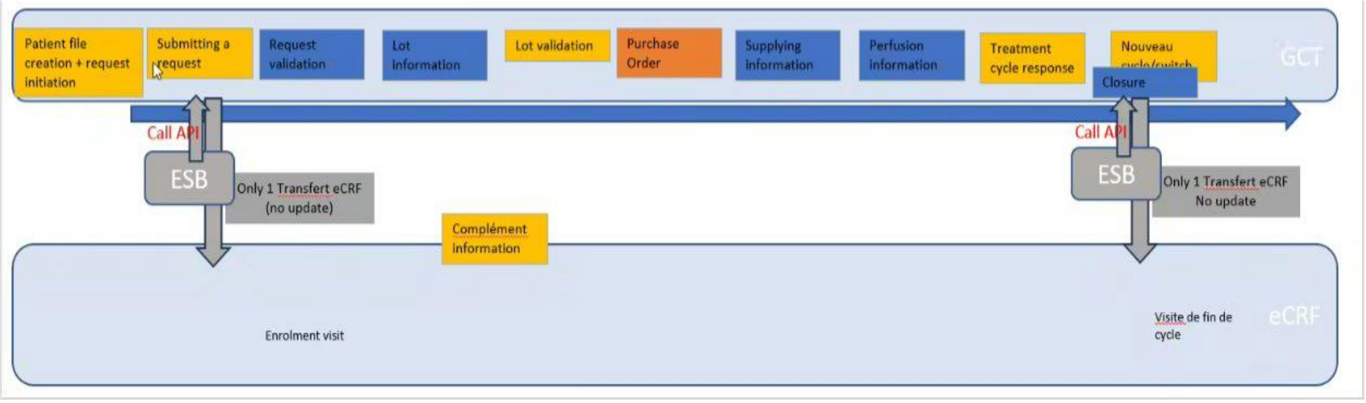
How does the life cycle of data and processes work?

Information gathered in the GCT portal (prior to the study)

1. Upon a request from a treating physician to PFM, PFM will collect the required subject personal data from the physician.
2. The treating physician enters the required subject personal data into PFM's data collection portal.
3. Pierre Fabre cases manager will then enter the coded subject personal data into Atara's form within the Atara Case Management application (Appian).
4. This data entry initiates the cell matching process within Atara.
5. The subject data received in Atara Case Management then is transferred via manual data input by a trained Atara staff member to the Atara Cell Selection Module (TrakCel).
6. Once the lot selection is complete, a lot proposal form is transmitted via Atara Case Management from Atara to PFM.
7. PFM transmits the lot proposal form to the treating physician via their data collection portal. If further information is needed, the flow outlined above will repeat.

Data Importation from GCT portal to the EDC (ClinicalOne®) (secondary data)

The following scheme described the data flow from GCT- to the EDC (Electronic Data Capture).



Data transmission is conducted using a digital gateway, Application Programming Interface (API) Gateways and Enterprise Service Bus (ESB), using encryption mechanisms that ensure compliance with regulation and provide authenticity and confidentiality protection. The ESB ensure compatibility between systems and maintaining data flow without disruptions, this solution can maintain the data integrity.

Data transmission triggers – two times planned:

1) At enrolment visit, once the Principal Investigator requested the subject's treatment in GCT portal and subject agreed or did not object to use their personal data, enrollment data will be imported into the eCRF.

2) End of treatment cycle visit, subject response to treatment data will be imported. This will be done only if enrolment visit is completed.

Data abstraction from medical subject chart (primary data)

Principal Investigators (or authorized site staff) will abstract the additional information related to safety, effectiveness and all additional information not imported from GCT portal in the EDC, from the medical subject record. All data are collected as part of the routine medical care of subjects and as per the standard of care. No new data are generated from the study.

What are the data supporting assets?

GO CELL THERAPY : data interface between physicians and PFM.
Hermes (forecast tool)
ThermoFisher (logistic tool)

Process	Detailed description of the process	Data supporting assets	Recipient
Site selection Investigator / site contacts	Identifiable information of the investigators involved in the study	Sent by secured system and documented in Oracle CTMS	Global CRO
Development of the eCRF	Development of the eCRF with secure access by recipients (the authorized users receive an	EDC system (ClinicalOne)	Global CRO Sponsor (Viewing on the

Process	Detailed description of the process	Data supporting assets	Recipient
	individual identifier and creates their own password to access the EDC platform)	Database hostage	EDC the pseudonymised subject personal data) Sites/ Investigators (Data collection)
Data collection from GCT Portal & sites	Transfer of medical data From GCT portal to eCRF. eCRF completion with personal medical data extracted from subjects' medical records by the principal investigator and/or authorised site staff assigned by the principal investigator Pseudonymised subject personal data detailed in section (Study dates, demographic data, clinical data)	ClinicalOne ClinicalOne access secured by an individual password, access delivered only after training & signature of training log Access authorization based on the role & permission of the person.	Global CRO Sponsor (Viewing on the EDC the pseudonymised subject personal data)
Site data management	On-site monitoring conducted as part of a quality control of data collection, carried out by a qualified Clinical Research Associate (CRA), authorized to consult the subjects' medical records and the data entered in the eCRF Identifiable subject data and pseudonymised subject personal data.	ClinicalOne	Global CRO Involved in the data review / data management Sponsor (Viewing the pseudonymised subject personal data)
Data Management	Manual and automatic queries generated for data verification and/or validation with the principal investigator, protocol deviation) Pseudonymised subject personal data	eCRF / ClinicalOne	Sites/ Investigators (Queries resolution)
Data Medical Review	Data medical review will be carried out in collaboration with the Sponsor. Pseudonymised subject	Database hosted in ClinicalOne	Global CRO Sponsor (Viewing on the EDC the pseudonymised

Process	Detailed description of the process	Data supporting assets	Recipient
	personal data		subject personal data)
Statistical analysis	As per statistical analysis plan (SAP). Pseudonymised subject personal data	SAS software Statistical TFL sent by secured system (Sharepoint)	Global CRO Sponsor Statistical TFL review
Database transfer	Study database	Statistical tables sent by secured system (sFTP Platform)	Sponsor
Clinical study report	Clinical study Report written as per STROBE guidelines Aggregated and anonymized subject personal data (study dates, demographic data, clinical data)	Sent by secured system (Sharepoint)	Sponsor Regulatory Authorities, when applicable

Fundamental principles

This section allows you to build the compliance framework for privacy principles.

PROPORTIONALITY AND NECESSITY

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

Are the processing purposes specified, explicit and legitimate?

PFM exclusively collects data for specified, explicit and legitimate purposes to better characterize the safety and effectiveness of the of tabelecleucel in subjects with EBV+ PTLD following Hematopoietic Cell Transplantation (HCT) or Solid Organ Transplantation (SOT).

What are the legal basis making the processing lawful?

The data subject has given consent to the processing of his or her personal data for one or more specific purposes in countries the Article 6.1.a of GDPR applies as per local regulation or local Data Protection Authority recommendation. This is applicable for lots of EU countries, except when consent waiver is applicable as per local regulation for data abstracted from subject medical chart.

For France, the lawfulness is based on Article 6.1.f., the processing is necessary for the purposes of the legitimate interest pursued by PFM.

For Italy , as independent controller, the lawfulness of processing carried out by the participating sites is the Article 6. 1. e of the Regulation for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For living subject, the subject has given consent to the processing of their personal data for one or more specific purposes as per the Article 6.1.a of GDPR

Given the impossibility or disproportionate effort of obtaining subject consent for this study due to the nature of the study with the inclusion of deceased, no longer traceable subjects, there is a possibility to use the legitimate interest as legal basis (Article 6.1.f.).

For such patients (deceased or no longer traceable or alive subjects without the impossibility to get their consent during the study period), the participating sites will be required to document in the medical record of the subjects the reason for the impossibility of obtaining consent and any description of the attempts made to contact the subjects and therefore the impossibility to contact them.

Additionally, it should be clarified that the processing of personal data in this study is necessary for scientific purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, pursuant to Article 9. 2.j. of the Regulation and in accordance with Article 110 of Legislative Decree 196/2003 in Italy.

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

The subject and the HCP personal data collection is limited to what is strictly necessary in order to answer the study objectives.

All dates (date of enrolment / date of consent form / information letter, date of diagnosis, dates of treatment, etc.) are recorded according in DD/MM/ YYYY format.

Subject vital status (cause of death and date of death) is needed to assess the efficacy of the treatment. A drop-down list is used (yes/ no questions) and date recorded in DD/MM/YYYY format.

Eligibility criteria required to ensure that subject is allowed to be included in the study as per regulation and protocol (Yes/No question).

Subject characteristics (age, gender, year of birth) are required to characterize the EBV+ PTLD subject population (paediatrics / older population). Year of birth recorded according to the following field (No full date of birth collected – YYYY). Gender recorded according to the following field: Male / Female.

Medical data collected via GCT portal and abstracted from medical subject record will serve to characterize the EBV+ PTLD subject population, describe the safety and effectiveness profile of these subjects. Drop-down list with pre-identified answers, lab values, dates in DD/MM/YYYY.

Are the data accurate and kept up to date?

Data quality controls in place :

Data quality controls	Justification
Study monitoring will be conducted by the local monitors. Study monitors from the Global CRO will perform ongoing source data verification (SDV) to confirm that critical protocol data (i.e., source data) entered into the eCRFs by authorized site personnel are accurate, complete and verifiable from source documents.	A Clinical Research Associate (CRA) from the CRO authorized to access to the medical records will come to the site to carry out the necessary data checks and report any deviations observed. A Monitoring Plan is developed for this study.
Manual or automatic queries throughout the data collection period.	The queries are generated via the EDC system and can be accessed securely by the principal investigator and staff authorized to connect to the platform.
EDC compliance with ICH GCP, 21 CFR Part 11 and GDPR requirements, including Traceability of records with audit trail timestamp	As part of Clinical One compliance.

What are the storage duration of the data?

Personal Data will be stored for a period consistent with the relevant regulatory requirements related to the study conduct in Europe including pharmacovigilance obligations (for at least 15 years).

Fundamental principles

This section allows you to build the compliance framework for privacy principles.

CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

How are the data subjects informed on the processing?

Consent (or assent for paediatric subjects or parent's consent for minors) will be obtained from all subjects except for France where it is not requested by local regulation. The participating physicians or the authorized site personnel will be responsible for providing the subject information documents and obtaining (when applicable) the consent of subjects meeting inclusion criteria. The consent will distinguish between consent to participate in a study and the requirements for lawful processing of personal data under the General Data Protection Regulation Compliance Guidelines.

The data privacy agreement required for providing treatment is distinct from the consent required for participation in the PASS. This agreement must be obtained prior to initiating a tabelecleucel inventory check and ordering the product.

The study consent includes:

- consent for secondary use of data collected in the HCP portal database
- consent for collection and use of primary data

The format and content of subject information letter and informed consent documents will adhere to IRBs/IECs requirements, applicable laws and regulations of the participating country, and will describe the nature, purpose, procedures, risks, and benefits of the study. Subjects will also be informed of their right to withdraw their consent at any time during the study without any consequences with respect to treatment. The participating physician will be responsible for obtaining subject consent. The database will contain safeguards to check whether consent has been obtained. The informed consent form will be provided to the participating physician in the Investigator Site File (ISF) and will be submitted to the Institutional Review Board/Independent Ethics Committee if required by local legislation.

Informed Consent Procedures for Specific Populations (minor, deceased and lost-to-follow-up) is considered for this study and described below:

Minor subjects

For all minor subjects living at the time of enrolment, a written consent or non-opposition from the appropriate legal representatives of these subjects will be obtained. Additionally, a written consent / assent or non-opposition will be obtained for the minor subjects able and legally authorized to consent/assent. The content of the study documents for minor subjects included in the study will be similar to the content of the adult documents and adapted according to the age groups specified by the local regulation.

Deceased subjects at the time of enrolment

Due to the nature of the study, subjects deceased at the time of enrolment can be eligible for the study. For all participating countries, the inclusion procedures of deceased subjects (adults and minors) must comply with the local regulation. This may include, for instance, informed consent waiver, confirmation that the subject (when alive) did not oppose to the use of medical data for research, or any other local regulatory requirements as applicable.

Lost-to-follow-up subjects at the time of enrolment

The participating centres will make every effort to contact, inform the subjects and will document this before considering the subjects to be lost to follow-up. The inclusion procedures of lost-to-follow-up subjects (adults and minors) must comply with the local regulation. This may include, for instance, informed consent waiver or any other local regulatory requirements as applicable.

If applicable, how is the consent of data subjects obtained?

Consent (or assent for paediatric subjects or parent’s consent for minors) will be obtained from all subjects except for France where it is not requested by local regulation. The participating physicians or the authorized site personnel will be responsible for providing the subject information documents and obtaining (when applicable) the written consent of subjects meeting inclusion criteria. The consent will distinguish between consent to participate in a study and the requirements for lawful processing of personal data under the General Data Protection Regulation Compliance Guidelines.

In France, according to the local regulation a signed Informed Consent is not required to enrol a subject in non-interventional studies. However, subjects should be adequately and individually informed in accordance with the provisions of Article 14 of the General Data Protection Regulation and French Data Protection Act (La loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés « Loi informatique et Libertés »). Notably, subjects should be informed that they may oppose to data collection at any point during the study and without any consequences on their ongoing care. Participating sites will send subject information letter via registered post with an acknowledgement of receipt. An opposition to the data collection expressed by subjects or their representatives at any point during the study is considered as withdrawal of the study.

For all country, the written consent will be obtained or the subject information letter will be sent prior to any data transfer (secondary data collection via GCT portal transfer) or data collection (primary data collection via medical subject record).

How can data subjects exercise their rights of access and to data portability?

The subject can exercise his/her rights by contacting his/her physician in priority, also by the site's Data Protection officer (DPO), or the sponsor through their DPO.

Data Portability: subjects can receive their personal data in a standardized electronic format for countries where the consent is the legal basis (Article 6.1.a). The data portability is not applicable for France.

How can data subjects exercise their rights to rectification and erasure?

Rights to rectification: No personal data can be modified directly by the subject in the e-CRF, but the modification of the collected data can be done if the subject requests it by e-mail, by mail to the investigator or/and the DPO of the site or/and the DPO of the Sponsor

Rights to erasure: The subject can exercise his or her right to erase their personal data by sending a request to the investigator or/and the DPO of the site or/and the sponsor's DPO. The request will be analysed by the sponsor in collaboration with the Global CRO, according to the type of data the subject wishes to delete, to evaluate the possible impact on the analysis which could lead to bias and compromise the research.
Depending on the type of data, some data could be deleted, others not. Subjects will be informed if their data can be deleted or not and the reason why not.

This evaluation is possible because the processing is necessary for scientific research purposes in accordance with Article 89(1).

How can data subjects exercise their rights to restriction and to object?

The subject can exercise his/her rights by contacting his/her physician in priority, also by the site's Data Protection officer (DPO), or the sponsor through their DPO.

Are the obligations of the processors clearly identified and governed by a contract?

A service agreement was signed on 12 July 2023 between PFM and Cerner Enviza France (now Oracle France SAS), including the GDPR contractual provisions, and a Data Security Agreement considering PFM is the Data Controller and Oracle France SAS is the Data processor.

In the case of data transfer outside the European Union, are the data adequately protected?

Yes by the conclusion of Standard Contractual Clauses as enacted by the European Commission (June 2021 edition)

Risks

This section allows you to assess the privacy risks, taking into account existing or planned controls.

There are no medical related risks for taking part in the study. In particular, the study will not involve any changes in the standards of cares of the subject, does not compromise their physical or psychological integrity and does not require any special follow-up visits for these subjects.

However, the data processing may entail the privacy risk on subjects ‘rights and freedom with are detailed in the section “RISK ASSESSMENT: POTENTIAL PRIVACY BREACHES”

In order to minimize the risks deriving from the data process, PFM and the CRO have adopted a series of technical and organizational security measures to protect the processing of personal data in the context of the study, in accordance with pursuant to Article 89 of the GDPR, and the provisions and guidelines issued by the local privacy law, which include:

A Data security agreement as part of the services agreement between PFM and Oracle France SaS includes the security and organizational controls.

This Data security agreement include the following aspects:

- Security Manager
- Geographic location of services and data
- Production / non production environment
- Vulnerabilities and patches management
- Anti-Malware protection
- Back-up and recovery policy
- Sub-contracting
- Logical access control
- Data protection
- Communication protection
- Audit logs

Technical measures adopted by PFM and/or the CRO:

- The omission of Patients' identified data (i.e. name, surname, date of birth, etc.) from any report, publication or other disclosure, except where required by applicable laws;
- Security technique to protect the sensitive data: all medical/ health data collected will be pseudonymised with a unique patient identification number of 9 digits (2 digits for the country code, 2 for the site and 5 for the enrolled subject). Only the investigator or authorised persons dedicated to the study within the investigating centre have a correspondence list with the patient identification number of 9 digits (PIN) and the patient's identity. Only authorised persons have access to this correspondence sheet and to the patient's medical records during the entire study period (CRA for monitoring, competent authorities). This correspondence sheet is in the study file, which is stored in a secure, locked location in the hospital and is only accessible by health care staff authorised to use the study file.
- The storage of Patients' personal data which have been pseudonymized in encrypted electronic form, protected by a password or in a locked room at the CRO research centre, ensuring that only expressly identified and authorised personnel have access to data;

- The recovery of personal data processed in the event of a catastrophe or any other event that may be qualified as a data breach.
- In the event of a potential or actual data breach, the CRO will be responsible for determining whether a data breach has actually occurred and, in such case, notifying PFM of the event, providing all information necessary to enable PFM to make the notifications required under Articles 33 and 34 of the GDPR, where necessary;
- The removal of identification data and/or any other data that identifies and/or makes identifiable Patients and the subsequent replacement of such data with a unique and specific numerical code in order to protect the Data Subjects' rights when data relating to the Study is communicated to other authorized parties;
- At the end of the data retention period, PFM has adopted the deidentification and anonymization techniques provided for in the "De-identification and Anonymization of Individual Patient Data in Clinical Studies;
- the adoption of adequate guarantees for the transfer of data, also outside the EEA, which allow PFM to maintain high standards of confidentiality and protection of Patients' personal data in accordance with Articles 44 and subsequent Articles of the GDPR.

In addition to the above, Oracle has adopted the specific Technical and Organisational Measures (TOMs) and policies which are:

Data protection policy: Oracle Corporate Security Practices September 2023 v3.2 (**Appendix 1**)

Oracle has an alert system for notifications of personal data breaches and security incidents: "information security incident response" page 8 of the "Oracle Corporate Security Practices September 2023 v3.2". Furthermore, a CHIA process (Complaint, Hazard, Incident, Accident) is in place that covers handling of data incident and data breach. All events are logged into JIRA software to keep track of the outcome.

Oracle® Life Sciences Clinical One Cloud Service (Clinical One) fulfils all criteria of complying with the FDA 21 CFR Part 11 regulatory demands ICH GCP described in *the OLS C1_Regulatory_Compliance_Addendum_V6_FINAL document* (**Appendix 2a**), and technical, organizational and procedure controls are in place to address the GDPR requirements (**Appendix 2b**). The data hosted once captured by Clinical One is located in Germany.

PLANNED OR EXISTING MEASURES

This section allows you to identify controls (existing or planned) that contribute to data security.

Cooling and Environmental Controls

- Temperature and ambient humidity is maintained per ASHRAE 9.9 standards
- Redundant (N+1) cooling system; includes direct-expansion systems with air cooled condensers and central stations with water-cooled chillers provide cooling in the computing area
- Water detectors are located in the under-floor space, where applicable
- Humidity is monitored throughout Salesforce's data center space

Physical Access Control Policies

- Access requests must be approved by a member of the Technical Operations team and tracked via an internal tracking system case.
- All persons must present government-issued photographic identification (e.g., driver's license) to the security reception personnel, who then issue access cards or visitor badges

- Visitors must be escorted to the Salesforce dedicated space by Salesforce personnel or data center security
- Only authorized Salesforce Technical Operations employees have physical access to the production systems. These personnel must register in the biometric scanning system prior to use
- Only authorized Salesforce personnel have access to Salesforce dedicated spaces. Access is additionally restricted based on job function
- Employee access is immediately rescinded in event of termination of employment or transfer to other duties
- Non-employee access (such as vendors) to the Data Center must be scheduled in advance by Technical Operations and are required to present valid government-issued photo identification and sign a log on arrival
- After appropriate checks, non-employees, who are supervised by Salesforce full time employees, may be given access to Salesforce space to time-bound projects
- Access logs are retained for a minimum of 90 days
- Salesforce Technical Operations reviews the access records (logs and authorized access lists) quarterly

Physical Access Control Procedures

- The Data Center lobbies have 24-hour dedicated physical security personnel on-site, with a man-trap entrance
- The route from the data center entrance to physical server access requires multiple security challenges, including a combination of two-factor biometric scans
- An alert is logged with security with each failed attempt
- Locked-out users must notify Security of the failure in order to regain access
- The Salesforce production systems are housed in dedicated, secure space separate from the rest of the Data Center, which requires biometric scan and badge or pin pad access to enter.
- Salesforce employees and vendors must return access badges to data center security upon departure
- All persons are subject to search upon entry and before leaving the facility Salesforce uses colocated data centers to host our production environment. Salesforce operates a primary data center and a failover data center for each instance of our service, in case there is a catastrophic failure of the primary data center. There are additional facilities used as test environment/labs. Only authorized Salesforce Technical Operations employees have access to these facilities.
- Salesforce systems that deliver the solution are contained in a dedicated, secure space separate from the rest of the Data Center. The cages within the room extend to the overhead cable trays. Motion sensors and cameras aimed at this level detect any movement and trigger alerts to security surveillance.

Additional Facility Controls

- Restricted access controls are in place to protect entry into the Meet-Me location, a segregated area for external connections between the Salesforce systems and the carrier circuits. Access to this space is limited to collocation data center staff
- All points of entry (e.g., roof, manhole, utility and network vaults, doors) are monitored
- Interior and exterior video surveillance with motion sensors on key areas to detect activity. Video is stored on disk and retained for a minimum of three (3) months
- Third-party security patrols throughout the facility and external grounds
- The shipping/receiving area is physically isolated from the computing area. Shipping/receiving is monitored by video, the access to the data center floor is restricted and managed by collocation data center staff
- The use of all photographic, video, audio and other mobile recording devices is prohibited in secure areas unless authorized

Cooling systems maintenance

- Cooling systems are maintained and tested per OEM (manufacturer's recommendations)
- Building engineered for local seismic, storm, and flood risks
- Located above sea level with no basement and a drainage/evacuation system

Power

- Underground utility power feeds. All electrical switching is inside the building, and these areas are accessible only to data center authorized personnel
- Communications and server rooms have two independent power sources.
- Redundant (N+1) generators
- Redundant power distribution units (PDUs)
- Redundant (N+1) UPS systems

- On site fuel storage provides minimum 24 hours runtime at full load in the event of a disaster
- Data centers retain contracts with multiple refueling providers

Data Replication

At Salesforce, trust is our #1 value and our data center strategy supports the company's commitment to run the most secure, trusted, reliable, and available cloud computing service. Customer success drives our data center strategy and delivering the highest standard in availability, performance, and security is our top priority. To that end, we build and serve each Salesforce instance from two geographically diverse data centers to avoid single points of failure in our infrastructure. This design supports the continuous availability our customers have come to expect from us.

At any given time, your Salesforce instance is actively served from one location with transactions replicated in near real-time to a completely redundant, secondary location. We regularly site switch between the locations for maintenance, compliance, and disaster recovery purposes. As we continue to expand and improve our global infrastructure presence, we recommend customers build their applications free of specific data center requirements to support a seamless Salesforce experience.

In addition, we have instances served from Amazon Web Services (AWS) Cloud infrastructure in the United States, Canada, India, and Australia. These instances are located in two or more separate Availability Zones within each respective country.

Please refer to this knowledge article for information on how to determine where your instance is located:
https://help.salesforce.com/articleView?id=Where-is-my-Salesforce-instance-located&type=1&mode=1

Systems Maintenance

- Colocated data centers test and maintain their power systems according to industry standards at minimum.
Network
- Concrete vaults for fiber entry
- Redundant internal paths
- Network neutral; connects to major carriers

Fire Suppression

- VESDA (very early smoke detection apparatus) sensors are installed throughout the data center and sampling points in the air handling systems
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression limits response only to affected area(s)
- Smoke detectors are deployed at the ceiling level and under the raised floor throughout the co-located data center facilities
- All fire suppression systems are inspected either in-house by colocation data center staff or by OEM personnel according to manufacturer's recommendations
- Manually operated fire extinguishers are in place throughout the facility and inspected per the OEM standards and annually at minimum Monitoring The data center engineering staff provides 24-hour monitoring in the Operations Center
- Data Center personnel have the capability to remotely monitor all data center environmental systems.
Emergency Action Plan Each of the colocated data centers have a documented Emergency Action Plan.
- Data center employees are trained in the execution of the plan
- The plan includes contact information for local emergency services

Physical Access Policies

Salesforce maintains a formal company-wide information security management system (ISMS) that conforms to the requirements of ISO 27001, including security policies, standards, and procedures. Formal policies, procedures, and job descriptions are documented for operational areas including: data center operations, development, program management, production management, infrastructure engineering, quality engineering, release management, operations, hiring, and terminations. These policies and procedures have been developed to segregate duties and enforce responsibilities based on job functionality.

Physical Access Communication

Salesforce reviews all user access across systems, applications, and databases at least every 90 days. Contractor access is reviewed 90 days after provisioning and requires re-approval by the approving manager to continue or terminate access.

Hardware maintenance

Salesforce leases most of its hardware for a period of three years, therefore hardware refreshes occur at minimum once every three years. However, as Salesforce receives tremendous benefits from advancements in technology due to its multi-tenant architecture, Salesforce often performs hardware refreshes on a shorter cycle.

Activity Continuation Plan

Salesforce has developed a global Business Continuity and Disaster Recovery Program for the Salesforce Services; hired Certified Business Continuity Planners (CBCP) and retained the services of leading consultants to assist in the on-going development of Business Continuity and Disaster Recovery plans and procedures. This program is overseen by senior management for each of the key functional areas within Salesforce, and is supported by executive leadership at the highest level.

Salesforce has a Crisis Management Team (CMT) comprised of select executives from key departments globally. The CMT is mobilized when a crisis or significant event occurs, and is responsible for evaluating the situation and responding accordingly. Depending on the severity and nature of an incident the CMT Leader may request engagement from various support teams to assist with mitigation of the incident. The CMT meets periodically for training, education, and review of the documented CMT Action Guide, or as required due to a crisis or significant event. CMT members have specified roles and responsibilities and are expected to be available at all times (24/7/365). The CMT conducts table-top exercises, at minimum of once annually.

Salesforce maintains a Mirror Site that is a 100% staged warm site with real-time (async) data replication. The secondary data center is replicated at 100% of capacity (host, network, and storage) of the Production data center. As part of developing a viable Disaster Recovery plan and program, Salesforce schedules Disaster Recovery exercises which are conducted several times per year. Salesforce will test its disaster recovery plan at minimum on an annual basis and will continue to enhance and develop processes and its technology related to disaster recovery to further reduce RPOs and RTOs. Salesforce has developed additional procedures, processes and plans, including a Pandemic plan.

Additionally, disaster communication processes are exercised using the mass notification system during each exercise, which includes call-outs with response requests to Salesforce Crisis Management Team and the production Disaster Recovery teams.

Power Supply and Communication

To maximize availability, the service is delivered using multiple world-class data centers supporting primary and replicated disaster recovery instances, plus a separate production-class lab facility. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance. The Salesforce Services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function.

Network Security

As per the Salesforce Network Protection policy:

- Networks must be segregated, either through logical and/or physical means. In addition to using separate physical devices, network architectures make use of security virtualization technologies to implement virtual networks, switches, interfaces, etc. These virtual network components isolate and protect network traffic to meet segregation requirements in this section.
- The network architecture defines subnetworks for publicly accessible system components that separate external traffic from traffic on internal Salesforce networks.
- Traffic must also be controlled and segregated based on functionality required and classification of the data/systems based on risks and respective security requirements.
- Segregation shall also be required between user functionality (e.g., web services) and information system management functionality (e.g., databases).
- Unless the risk is identified and accepted by the data owner, sensitive systems shall be isolated (physically or logically) from non-sensitive applications/systems.

- Zone and First Party Data Center-specific security controls
- All zones connected to untrusted networks (i.e., Internet, ISPs) must use an edge/border router for terminating links.
- To restrict traffic, ACLs or another strong security mechanism should be in place between edge / border routers and the internal routers in the data center.
- Edge / border routers should only be used for interfacing with ISPs and other transit providers.

Shared Network

Salesforce has implemented a zone-based network segmentation approach with firewalls and intrusion detection systems appropriately placed within each zone. External firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. Ingress traffic traverses an edge layer and a load-balancing layer before encountering the datacenter forwarding layer which routes requests as needed.

Salesforce network management policies defines protection mechanisms that includes:
- External network connections are routed through boundary protection mechanisms.
- Network topology diagrams are designed in a way to determine whether boundary protection mechanisms are in place to manage inbound and outbound external connections.
- Salesforce's network security standards defines requirements for routing external traffic through boundary protection mechanisms.
- Inspected access control lists (ACLs) or firewall rules on a selection of network devices is used to determine whether or not external traffic was routed in accordance with the Salesforce's production network security standard.
- Approved networking ports and protocols are implemented in accordance with the documented production network standards.

Vulnerability Management and Patch

Salesforce has a policy in place in which periodic vulnerability scans are performed on all Salesforce information system and hosted applications. Frequency and comprehensiveness of scans is defined by security categorization of the system, data sensitivity and/or specific regulatory requirements. Many of these scans are performed on at least a monthly basis across Salesforce products. Automated mechanisms are employed to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Vulnerability scan reports and results from security control assessments are analyzed and when new vulnerabilities potentially affect the system/application; they are identified and reported.

- Vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process shall be deployed by using standards for:
- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and

- Measuring vulnerability impact.

Identified vulnerabilities are assigned on priority basis with an associated internal service level agreement for remediation based upon risk. Salesforce management reviews vulnerability and patching status on a bi-weekly basis. Patches are deployed for known vulnerabilities at least monthly, or as need based on the criticality.

Virus and Malware Control

Salesforce has implemented malware detection at the network level in the production environment. Specifically, network intrusion detection systems are configured (and continuously updated) to detect malware-related network traffic. Other controls are also used to address malware such as hardening the Operating System of our UNIX and Linux-based servers and firewall configuration to ensure only required ports are open and all others denied. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real time through a security monitoring system. Salesforce does not restrict the file types users can upload. Salesforce does not scan, modify or clean any customer data; the system stores the information provided in an encoded format within the database. It is recommended that customers run updated antivirus and anti-malware solutions to help mitigate these threats. The production system receives inbound mail as part of the workflow functionality, but as the architecture of the system does not allow code in the email to be executed or transferred, this does not pose any threat to our network, application, or users. Email sent from the Salesforce application is not currently scanned for viruses. Customers can implement partner products such as WithSecure (also known as F-Secure) Cloud Protection for Salesforce to provide additional malware security for uploaded content.

Please see H&T article here (section on File Upload) for further information-
https://help.salesforce.com/s/articleView?id=000318378&type=1#FileUpload

Salesforce enforces anti-malware software installation on employee workstations and corporate servers. Malware definition parent servers check for updates daily and push updates to end user workstations and servers, which are configured to prevent end-users from permanently disabling anti-malware scanning. Alerts are generated in the event of compromise or potential compromise. Privileged access to the managed anti-malware server is restricted to system administrators.

Staging/Production platform segmentation

There are a limited number of Salesforce's Technical Operations employees with logical access to systems. These privileged users must authenticate to the Production Remote Access (PRA) gateway system. The PRA system hosts a secure environment in which the privileged users manage the production systems with the users receiving only a bitmap representation of a virtual screen hosted in the secure environment. Those with privileged access are required to authenticate to a secure server using 2 layers of two factor authentication.

Additional controls include:

- Management applications are not run locally on workstations
- Users cannot copy-paste data from the hosted environment
- Users are only able to launch two pre-approved applications: a Web browser (with limited Internet access) and a terminal.
- SSH is permitted only via the bastion hosts
- Internet connections from the client are allowed only via authenticated, logged proxies
- IM, email/webmail and any other Corp IT provided services are prohibited
- Administrative accounts are managed centrally, via TACACS+/Kerberos as well as by a two-factor authentication system
- Privileged users must log in using unique user IDs
- Generic/shared accounts are only accessible via sudo, and these events are logged centrally

Access Administration:

Technical Operations approves login/network access to servers and other infrastructure equipment. Administrative accounts are automatically locked after 90 days of inactivity and require a password reset by an administrator. Upon termination, privileged accounts are locked in Kerberos, connections are terminated and tokens are removed. Outstanding VPN/jumphost connections are terminated as well. If a user is transferred but will keep non-privileged access, administrative privileges are revoked centrally. Termination tasks are automatically triggered upon notification from HR. Logical access is reviewed quarterly by Technical Operations management.

Change Control

Salesforce: A formal Patch Management Procedure is a part of the Salesforce Change Management process that is focused on maximizing uptime and minimizing service downtime by confirming that changes related to upgrades, patches, and security fixes released by vendors are formally documented and evaluated.
The Change Management process requires that requests for changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner. System administrators evaluate changes in order to determine criticality for the production environment.

Modis: In our defined process, several environments are available & a ticketing tool is set to reference all functionnalities & changes. Each part of documentation is updated based on information available in our tool. Also, an environment (INT) is used by Modis team to validate developments. Second environment (Recette/UAT) is used by Modis & Pierre Fabre teams to test & validate deployments. Once this test phase is performed, a formal "Go" to move to production is given by Pierre Fabre teams. All project components are stored in a repository to ensure source control. Each manual task is also referenced in a separate file & each task is performed on deployment.

Encryption

Information stored within the Multi-Tenant Database and Document Storage infrastructure is encrypted at rest within the file system.

Salesforce is aware that choosing to store sensitive, confidential, or proprietary data with any third party often prompts customers to more closely investigate both external regulatory and internal data compliance policies. As customers look at regulations such as PCI-DSS, HIPAA/HITECH, and FedRAMP through the lens of cloud-based service adoption, they typically take a pragmatic but conservative approach to data protection in the cloud. To facilitate more advanced Data at Rest Encryption requirements, Salesforce offers Shield Platform Encryption which provides customers the ability to provide their own keys in addition to encryption key lifecycle management features. Shield Platform Encryption is available as an add-on subscription for Enterprise, Performance, and Unlimited Editions. For more information please refer to the product documentation: https://help.salesforce.com/articleView?id=sf.security_pe_overview.htm&type=5

Securized Transfert of Data

All transmissions between the user and the Salesforce Services are secured using TLS 1.2 and encrypted using 256 or 128-bit key. The Services use International/Global Set Up SSL certificates with 2048-bit Public Keys. The list of supported cipher suites is available from the salesforce knowledge base: https://help.salesforce.com/articleView?id=000351980&language=de&mode=1&type=1

Securized Data Management

Salesforce runs on a multi-tenant architecture and data is logically segregated. This is a high-level explanation of the authentication process and how data is segregated between Organizations (i.e. customers).

-A user navigates to login.salesforce.com and logs into our service by entering their user credentials (user name and password). Salesforce then issues a secure session token to the user, which is sent back and forth by the browser with every request that is made to our service. This session token is mapped to what we call "user context" inside the Salesforce Services. User context includes the Organization the user belongs to and who the user is inside that organization.

The organization that the user belongs to is how data is encoded inside of the tables within Oracle, so every record of every table has a Base62 encoded Char 15 Organization ID. Every query created by our service includes a "where clause", which includes the: Organization ID and User ID. The Organization ID separates your data from other organization data and the User ID sets up the sharing model for what the user will be able to view within your Organization's space. For each rendered page, the service confirms that the session is valid by comparing the session token sent by the client to the token within the session state table.

If the session token does not match, the service automatically logs out the user. The application scripts automatically append to the SQL query the Organization ID and User ID to the where clause of the query, retrieves the rows, validates that the rows still match the session that requested the rows, strips off the Organization ID and User ID, creates print statements and sends the requested data back to the browser and the page with the requested data is rendered.

Data Protection

Third parties contracted by Salesforce are required to commit to confidentiality agreements covering Customer Data. All third parties are subject to Salesforce policies and procedures as defined in the company Third Party Suppliers standard and other policies. This includes items such as background screening, training and breach of policy and enforcement. Prospective vendors supporting the production environment for the Salesforce Services are assessed for their security, compliance and privacy practices prior to signing contracts for services. These third-party vendors are also evaluated by the Salesforce compliance team prior to go-live. Deficiencies noted in the review are remediated and/or compensating control(s) identified to address key risks, prior to go-live with potential access to Customer Data. Contracts are in place with all third parties that support the production environment, and these third-party vendors are audited against SLAs and terms within their contract, including adherence to Salesforce policies and procedures and information and physical security practices on at least an annual basis.

Third Party committment

Third parties contracted by Salesforce are required to commit to confidentiality agreements covering Customer Data. All third parties are subject to Salesforce policies and procedures as defined in the company Third Party Suppliers standard and other policies. This includes items such as background screening, training and breach of policy and enforcement. Prospective vendors supporting the production environment for the Salesforce Services are assessed for their security, compliance and privacy practices prior to signing contracts for services. These third-party vendors are also evaluated by the Salesforce compliance team prior to go-live. Deficiencies noted in the review are remediated and/or compensating control(s) identified to address key risks, prior to go-live with potential access to Customer Data. Contracts are in place with all third parties that support the production environment, and these third-party vendors are audited against SLAs and terms within their contract, including adherence to Salesforce policies and procedures and information and physical security practices on at least an annual basis.

Back Up

Backup media are encrypted using a FIPS 140-2 compliant encryption module using AES256. Backups do not physically leave the Salesforce data centers and access is restricted to authorized personnel. Backups are kept in our secure, dedicated data center space until they are to be retired and destroyed.

Active customer data stays in storage until the customer deletes or changes it. Data deleted by the customer is then temporarily available in the application Recycle Bin for 15 days, after which the records are marked for deletion and are no longer available to users. Data marked for deletion is permanently deleted by batch jobs over a 90 day period after being marked for deletion. Both the customer data and data marked for deletion are retained on backup media for 90 days (30 days for sandbox instances).

Audit Log

Salesforce internal infrastructure logs are collected by various monitoring tools for activities on the systems that host Salesforce, and include:
- Server access
- Network access
- Firewall management events
- Network intrusion detection systems traffic (signature and anomaly based)
- Database
- File integrity
- Network device configuration

Log events are correlated to generate alerts. Alerts are configured to notify the Technical Operations and Computer Security Incident Response Team (CSIRT) teams. Security alerts require acknowledgement and follow up, if appropriate by the CSIRT. Firewalls and IDS systems are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of (1) one year. Infrastructure Logs are scrubbed of Personal Data that is part of Customer Data before being stored in the central logging infrastructure.

Infrastructure logs are collected and stored in a log management system that is managed by the Salesforce Security organization. Users of this system do not have the ability to modify or delete log data. Administrative access to this environment is limited to a small number of authorized individuals within the Security organization.

Logs Revision

Infrastructure logs are collected and stored in a log management system that is managed by the Salesforce Security organization. Users of this system do not have the ability to modify or delete log data. Administrative access to this environment is limited to a small number of authorized individuals within the Security organization. Salesforce's Computer Security Incident Response Team (CSIRT) uses a security event logging and management system to manage the security alerts and logs generated by devices on our network. The system consists of a central database, management server, and distributed agents. The distributed agents receive events from network devices and systems (firewalls, IDS, routers, switches, hosts, file integrity, and database monitoring) on the network, the compress, encrypt, and transmit the data to the management server and database for processing. Correlated events are configured to generate alerts and logs which are monitored on a 24/7 basis. Firewalls and IDS systems are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of 1 year.

Encrypted Communication

All transmissions between the user and the Salesforce Services are secured using TLS 1.2 and encrypted using 256 or 128-bit key. The Services use International/Global Set Up SSL certificates with 2048-bit Public Keys. The list of supported cipher suites is available from the salesforce knowledge base:
https://help.salesforce.com/articleView?id=000351980&language=de&mode=1&type=1

Users Authentification

Salesforce provides several methods to authenticate users. Some methods are automatically enabled, and some require that you enable and configure them.
Single sign-on and two-factor authentication may be used to authenticate users. Salesforce has its own system of user authentication, but some companies prefer to use an existing single sign-on capability to simplify and standardize their user authentication. There are two options to implement single sign-on: federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by

organization. The primary reasons for using delegated authentication include: - Using a stronger type of user authentication, such as integration with a secure identity provider - Making your login page private and accessible only behind a corporate firewall - Differentiating your organization from all other companies that use Salesforce in order to reduce phishing attacks You must request that this feature be enabled by Salesforce. Contact Salesforce to enable delegated authentication single sign-on for your organization. Authentication providers let your users log in to your Salesforce organization using their login credentials from an external service provider. Salesforce supports the OpenId Connect protocol that allows users to log in from any OpenID provider such as Google, PayPal, LinkedIn and other services supporting OpenID Connect. When authentication providers are enabled, Salesforce does not validate a user's password. Instead, Salesforce uses the user's login credentials from the external service provider to establish authentication credentials. This information was obtained from the following Help & Training article:
https://help.salesforce.com/HTViewHelpDoc?id=security_overview_auth.htm

RISK ASSESSMENT: POTENTIAL PRIVACY BREACHES

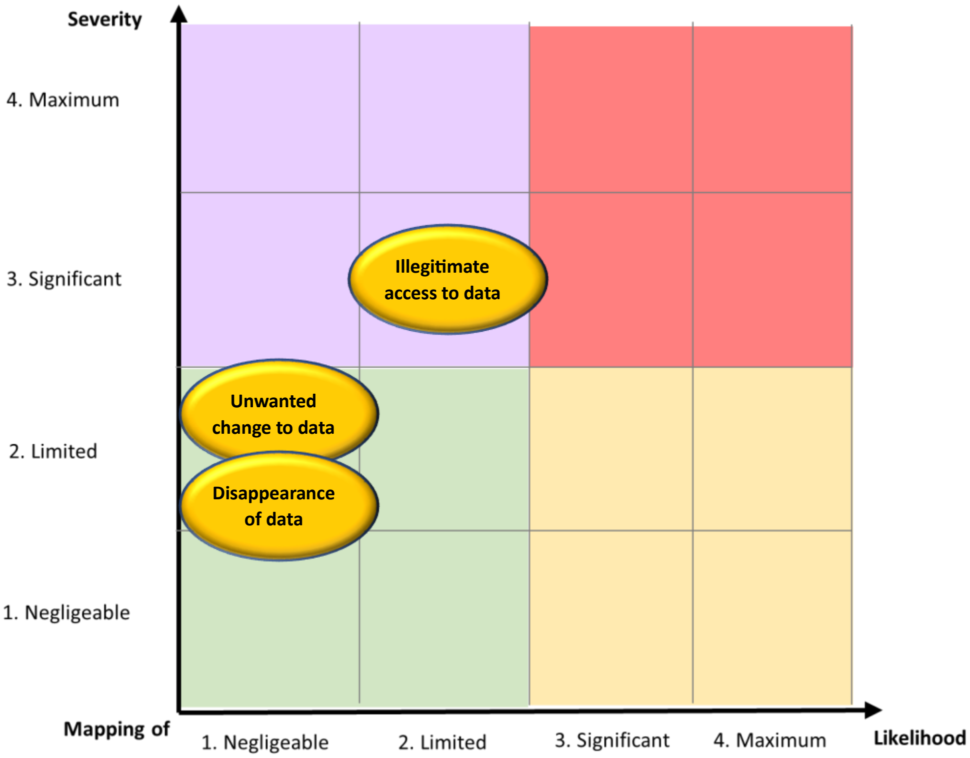
Analysis and assessment of risks

Risk	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Illegitimate access to data	Investigator Unauthorized persons	Personal Data processing without the knowledge of the risk of data breach Accidental disclosure Cyberattack Data stealing	Failure to respect the rights and freedoms of the subject. For example: feeling of invasion of privacy with irreversible damage, feeling of violation of fundamental rights (e.g. discrimination, freedom of expression), cyberbullying and harassment.	Awareness & training at site initiation and during the course of study through monitoring visits and/or communication No direct identifying data collected (surname, first name, email, address, etc.) that can be used to re-identify the subject. Encryption measures for data hosted and storage Limited access to files with a limited lifespan.	Significant	Limited

				Organizational measures (staff authorization, relations with third parties)		
Unwanted change of data	Human mistake (internal employee) Failure in IT system	Accidental data alteration	Need to collect the corrected data from subject records (kept in a secure place in the site) without re-identification of the subject	Since all data are stored in the clinical database with audit trails, edits checks and manuals queries are raised by monitoring, data management, safety and medical review. Most of the data collected during the Study are saved in the clinical database maintained by processors working on behalf of the sponsor, the Data Controller. These processors have their own security measures. At the end of the study, personal data collected in the clinical database are archived. Meaning that the database is locked which renders	Limited	Negligeable

				impossible any modification of data.		
Disappearance of data	Human mistake (internal employee) Failure in IT system Disaster: destruction of servers	Accidental deletion / disappearance of data	There is existing control in place at to limit the threats. Some of these measures are improvable to increase the level of data protection regarding the data disappearance. All the personal data collected during the clinical trial and entered in the clinical database are entered by a study nurse using source documents available on site. In case of data disappearance, the risk for data subjects is negligeable since the database might be rebuild based on the source documents	IT security and safeguard in place. Organization procedures (staff authorization, relationship with a third party) Traceability (access log) General system security procedures (operation security and workstation management) Protection against non-human sources of risk in place Data incident /data breaches management with the implementation of an alert procedure. Depending on decision related to the data incident/ data breaches, the subjects or their legal representative must be informed	Limited	Negligeable

Mapping risks related to data security



Data workflow chart

The data workflow chart of Ebvolve study is described in the **Appendix 3**

FORMAL VALIDATION OF THE DPIA

In light of the information provided in this document and given the modalities of the data processing described above, the Data Protection Officer agrees with the Sponsor's assessment.

The purpose of the processing is the scientific research and public interest to describe and characterize the safety and effectiveness profile of tabelecleucel in subjects with EBV+ PTLD following Hematopoietic Cell Transplantation (HCT) or Solid Organ Transplantation (SOT), in a real-world setting in Europe.

The measures foreseen to respect the fundamental principles of privacy and to address the risks to the privacy of the subjects are indeed considered acceptable in view of this issue. However, the implementation of additional measures will have to be demonstrated, as well as the continuous improvement of the DPIA.

Pierre-André POIRIER, Data Protection Officer

08-juil.-24 | 13:44:31 CEST

DocuSigned by:

POIRIER Pierre Andre

Nom du signataire : POIRIER Pierre Andre
Motif de la signature : J'approuve ce document
Heure de signature : 08-juil.-24 | 13:44:17 CEST
EB9EFD9AD54B461DA8F37002AF5FBD60

APPENDIXES

Appendix 1: Oracle Corporate Security Practices September 2023 v3.2

Appendix 2: Oracle® Life Sciences Clinical One Cloud Service (Clinical One) documentation

- **Appendix 2a**: OLS C1_Regulatory_Compliance_Addendum_V6_FINAL
- **Appendix 2b**: Technical, organizational and procedure controls (Oracle_Life_Sciences_Clinical_One_Cloud_Service_Product_Service_Feature_Guide_July_2023)

Appendix 3: EBVOLVE_Data workflow chart_20240320

Appendix 4: Go Cell Therapy DPIA