VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Contesto

Questa sezione fornisce una visione chiara del trattamento dei dati personali in questione.

PANORAMICA

Questa parte consente di identificare e presentare l'oggetto dello studio.

Qual è il trattamento in esame?

Lo studio EBVOLVE è uno studio osservazionale, multicentrico e multinazionale sulla sicurezza post-autorizzazione (PASS).

Questo studio è condotto esclusivamente a scopo di ricerca scientifica e di interesse pubblico per descrivere e caratterizzare il profilo di sicurezza e di efficacia di tabelecleucel in soggetti con PTLD da EBV+ dopo trapianto di cellule ematopoietiche (HCT) o trapianto di organi solidi (SOT), in un contesto reale in Europa.

Lo studio è stato commissionato dall'Agenzia Europea dei Medicinali (EMA) e il protocollo dello studio è stato approvato dal Comitato di Valutazione dei Rischi per la Farmacovigilanza (PRAC), il comitato dell'Agenzia Europea dei Medicinali (EMA) responsabile della valutazione e del monitoraggio della sicurezza dei farmaci per uso umano. Durante la revisione della domanda di autorizzazione all'immissione in commercio di tabelecleucel, l'EMA ha richiesto la raccolta di dati aggiuntivi sulla sicurezza e l'efficacia di tabelecleucel, compresi gli esiti a lungo termine, in particolare nelle popolazioni pediatriche (età < 18 anni) e anziane (età ≥ 65 anni) a causa delle limitate evidenze disponibili. Questo protocollo PASS affronta le limitate evidenze in queste popolazioni speciali (pediatrici e anziani) e caratterizzerà ulteriormente la sicurezza e l'efficacia a lungo termine di tabelecleucel nell'intera popolazione di soggetti con PTLD EBV+ in un contesto reale, in conformità con le linee guida dell'Autorità Sanitaria Europea per i medicinali per terapie avanzate.

Quali sono le responsabilità legate al trattamento?

Pierre Fabre Medicament S.A. con sede legale in Les Cauquillous, 81 500 Lavaur, Francia (PFM) è lo sponsor e il titolare del trattamento dei dati . Altri responsabili del trattamento sono :

- Fornitori terzi di Pierre Fabre in qualità di responsabili del trattamento dei dati: SalesForces come fornitore e hoster del portale Go Cell Therapy.

- Oracle France SaS (e le sue affiliate), CRO global con sede in Francia, è incaricata da PFM di fornire i servizi completi per la conduzione dello studio (documenti dello studio, impostazione e gestione dell'EDC, attività di avvio, raccolta dei dati, gestione dei dati, analisi statistica, relazione sullo studio clinico, Trial Master File attraverso il sistema PFM, archiviazione) e di condurre le attività di studio in loco nei Paesi europei. Oracle France SaS e le sue affiliate agiscono come responsabili del trattamento dei dati.
  Oracle è responsabile dello sviluppo dei moduli elettronici per i rapporti sui casi (eCRF) attraverso il sistema di acquisizione elettronica dei dati, denominato Oracle® Life Sciences Clinical One Cloud Service (Clinical One). Questo sistema è stato sviluppato e progettato per l'inserimento dei dati online, la gestione e la convalida dei dati per gli studi clinici.

- I centri ospedalieri con sede in Europa, che ospitano i dati sanitari raccolti, le cartelle cliniche personali e altre informazioni personali identificabili relative al soggetto, a seconda delle normative dei Paesi dell'UE, sono considerati titolari del trattamento indipendenti o responsabili del trattamento. . Gli sperimentatori principali e il personale autorizzato delcentro, dipendente deicentri , saranno incaricati di attivare l'importazione dei dati dal portale Go Cell Therapy (GCT) alle eCRF tramite Oracle ClinicalOne, e saranno responsabili dell'estrazione dei dati dalla cartella clinica del soggetto (dati primari) e della documentazione della eCRF tramite ClinicalOne.

Esistono norme applicabili al trattamento?

Il regolamento europeo n. 2016/679, noto come Regolamento generale sulla protezione dei dati (GDPR), è in vigore dal 25 maggio 2018.

Leggi locali sulla protezione dei dati in ogni paese dell'UE coinvolto nello studio, se applicabili.

Specificità dell'Italia:

Il 23 aprile 2024, il Parlamento italiano ha approvato un emendamento al Codice della privacy relativo all'articolo 110 in materia di " “Ricerca medica, biomedica ed epidemiologica”.
Più precisamente, è stato abrogato l'obbligo per gli Sponsor di consultare preventivamente l'Autorità Garante per la Protezione dei Dati Personali (Garante) e ottenerne il parere prima di condurre studi che comportino il trattamento di dati sanitari a fini scientifici, ~~e~~ quando sia impossibile ottenere il consenso dei pazienti, o informare gli interessati sia "impossibile" o comporti "uno sforzo sproporzionato" o rischi di "impedire o danneggiare gravemente il raggiungimento degli obiettivi della ricerca".

Nonostante sia venuto meno tale obbligo, PFM ha messo in atto misure adeguate per proteggere i diritti, le libertà e gli interessi legittimi degli interessati prima del trattamento dei dati personali:

- La Valutazione d'Impatto sulla Protezione dei Dati sarà pubblicata sul sito di PFM e comunicata al Garante.
- Lo studio sarà esaminato e approvato dal Comitato Etico competente in Italia.
- I Pazienti ricevono l'Informativa sulla privacy ed esprimono il loro consenso al trattamento dei dati personali firmando il modulo di consenso informato
- Per i pazienti che hanno perso il follow-up, i centri compionosforzi ragionevoli per ottenere il loro consenso contattandoli all'ultimo indirizzo conosciuto. Il centrolo riporta nelle cartelle cliniche dei pazienti.
- Per i pazienti deceduti e per quelli ~~Lost-to-follow-up~~ non raggiungibili, poiché ciò comporterebbe uno sforzo sproporzionato o il rischio di mettere a repentaglio lo scopo dello Studio ai sensi dell'articolo 14, paragrafo 5, e del considerando 62 del GDPR, verrà pubblicata un'informativa sul sito web di PFM e sul sito web delCentro, nonché affissa nella sala d'attesa delcentro, quando possibile, consentendo ai rappresentanti legali, tutori, pazienti non raggiungibili per il follow-up diavere accesso all'Informativa sulla privacy ed esercitare i propri diritti.

Specificità della terapia cellulare GO

GO Cell Therapy (portale Salesforce) ASIP
Santé HDS
C5 ISAE 3000 (rivisto)
FISC (Giappone)
HiTrust IRAP
ISO 27001, ISO 27017, ISO 27018
NEN 7510-1:2017
PCI-DSS
SOC 1 Tipo II (Rapporto SSAE 18)
SOC 2 Type II (Trust Principles Report) TRUSTe
Certified Privacy Seal FedRAMP (NIST 800-53),
Marchio PrivacyMark del JIPDEC

Per maggiori dettagli, è possibile consultare il sito web https://compliance.salesforce.com/.

È stata sviluppata una valutazione d'impatto sulla protezione dei dati relativa alla GO Cell Therapy (portale Salesforce), riportata nell'Appendice 4.

Contesto

Questa sezione fornisce una visione chiara del trattamento dei dati personali in questione.

DATI, PROCESSI E ASSET DI SUPPORTO

Questa parte consente di definire e descrivere in dettaglio l'ambito dell'elaborazione.

Quali sono i dati trattati?

Tipi di dati	Destinatari
Informazioni identificabili di appaltatori, agenti, consulenti, come CRO, che gestiscono ed eseguono lo studio EBVOLVE (nome completo, dettagli di contatto), compresi i contratti (MSA/SOW), fatture, documenti amministrativi che devono essere conservati anche dopo la fine dello studio in caso di richiesta di audit/ autorità di regolamentazione.	PFM (Sponsor) Oracle France SAS (CRO global)
Informazioni identificabili degli sperimentatori principali e degli altri operatori sanitari coinvolti nello studio EBVOLVE (cognome, nome, titolo, e-mail professionale, indirizzo postale e numero di telefono, curriculum vitae, numero di licenza). Centrimedici : coordinate bancarie	PFM (Sponsor) Oracle France SAS (CRO global)

Tipi di dati	Destinatari
Dati anagrafici del soggetto pseudonimizzati: Anno di nascita, età, sesso alla nascita	PFM (Sponsor) Oracle France SAS (CRO global)
Dati sanitari del soggetto pseudonimizzati: anamnesi della malattia, caratteristiche del soggetto, PTLD da EBV+ alla diagnosi, anamnesi e tipo di trapianto, segnalazione di eventi alloreattivi in corso di trattamento, trattamento per PTLD da EBV+, esito del trattamento di base per ciclo di trattamento, informazioni sulla sicurezza.	PFM (Sponsor) Oracle France SAS (CRO global)

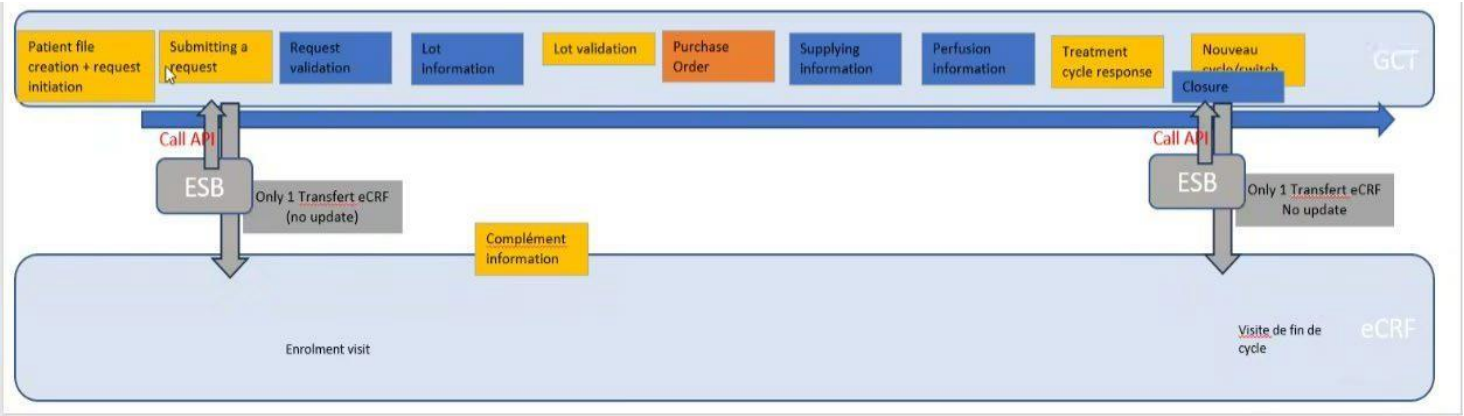
Come funziona il ciclo di vita dei dati e dei processi?

Informazioni raccolte nel portale GCT (prima dello studio)

1. Su richiesta di un medico curante ~~a~~l PFM, quest'ultimo raccoglierà i dati personali richiesti dal medico.
2. Il medico curante inserisce i dati personali del soggetto nel database di PFM (portale GCT).
3. Il *case manager* di Pierre Fabre inserirà quindi i dati personali codificati del soggetto nel modulo di Atara all'interno dell'applicazione Atara Case Management (Appian).
4. Questo inserimento di dati avvia il processo di abbinamento delle celle all'interno di Atara.
5. I dati dei soggetti ricevuti in Atara Case Management vengono poi trasferiti al modulo di selezione cellulare Atara (TrakCel) tramite l'inserimento manuale dei dati da parte di un membro del personale Atara appositamente formato.
6. Una volta completata la selezione del lotto, il modulo di proposta del lotto viene trasmesso da Atara Case Management a PFM.
7. PFM trasmette il modulo di proposta del lotto al medico curante tramite il portale di raccolta dati. Se sono necessarie ulteriori informazioni, il flusso descritto sopra si ripete.

Importazione dei dati dal portale GCT all'EDC (ClinicalOne®) (dati secondari)

Lo schema seguente descrive il flusso di dati dal portale GCT all'EDC (Electronic Data Capture).



La trasmissione dei dati avviene tramite un gateway digitale, gateway API (Application Programming Interface) ed ESB (Enterprise Service Bus), utilizzando meccanismi di crittografia che assicurano la conformità alle normative e forniscono protezione dell'autenticità e della riservatezza. L'ESB garantisce la compatibilità tra i sistemi e il mantenimento del flusso di dati senza interruzioni; questa soluzione può mantenere l'integrità dei dati.

Inneschi di trasmissione dati - due volte previsti:

1) Alla visita di arruolamento, una volta che lo sperimentatore principale ha richiesto il trattamento del soggetto nel portale GCT e il soggetto ha acconsentito all'uso dei suoi dati personali, i dati di arruolamento saranno importati nell'eCRF.

2) Alla visita di fine ciclo di trattamento, i dati di risposta al trattamento dei soggetti saranno importati. Questo verrà fatto solo se la visita di arruolamento è stata completata.

Estrazione dei dati dalla cartella clinica (dati primari)

Gli sperimentatori principali (o il personale autorizzato del sito) estrarranno le informazioni aggiuntive relative alla sicurezza e all'efficacia e tutte le informazioni aggiuntive non importate dal portale GCT nell'EDC, dalla cartella clinica del soggetto. Tutti i dati sono raccolti come parte delle cure mediche di routine dei soggetti e come da standard di cura. Lo studio non genera nuovi dati.

Quali sono i dati a supporto degli asset?

GO CELL THERAPY: interfaccia dati tra medici e PFM.
Hermes (strumento di previsione)
ThermoFisher (strumento logistico)

Processo	Descrizione dettagliata del processo	Risorse di supporto dei dati	Destinatario
Selezione del centro Contatti dello sperimentatore/sito	Informazioni identificabili degli sperimentatori coinvolti nello studio	Inviato da sistema protetto e documentato in Oracle CTMS	CRO global
Sviluppo dell'eCRF	Sviluppo della eCRF con accesso sicuro da parte dei destinatari (gli utenti autorizzati ricevono un	EDC sistema (ClinicalOne)	Sponsor CRO global (Visualizzazione su il
Processo	**Descrizione dettagliata del processo**	**Risorse di supporto dei dati**	**Destinatario**
	identificativo individuale e creano la propria password per accedere alla piattaforma EDC)	Database hostage	EDC dati personali pseudonimizzati del soggetto) Centri / Sperimentatori (raccolta dati)
Raccolta dati dal portale GCT e dai centri	Trasferimento dei dati sanitaridal portale GCT a eCRF. compilazione della eCRF con i dati sanitaripersonali estratti dalle cartelle cliniche dei soggetti da parte dello sperimentatore principale e/o del personale autorizzato del centroincaricato dallo sperimentatore principale dati personali pseudonimizzati dell'interessato dettagliati nella sezione (date dello studio, dati anagrafici, dati clinici)	ClinicalOne L'accesso a ClinicalOne è protetto da una password individuale, l'accesso è consentito solo dopo la formazione e la firma del registro di formazione. Autorizzazione all'accesso in base al ruolo e ai permessi della persona.	Sponsor CRO global (Visualizzazione sul CED dati personali pseudonimizzati del soggetto)
Gestione dei dati del centro	Monitoraggio in loco condotto come parte di un controllo di qualità della raccolta dei dati, effettuato da un Clinical Research Associate (CRA) qualificato, autorizzato a consultare le cartelle cliniche dei soggetti e i dati inseriti nell'eCRF Dati personali identificabili e dati personali pseudonimizzati.	ClinicalOne	CRO globalCoinvolta nella revisione dei dati/ gestione dei dati Sponsor (Visualizzazione di dati personali pseudonimizzati del soggetto)

Gestione dei dati	Query manuali e automatiche generate per la verifica e/o la convalida dei dati con lo sperimentatore principale, deviazione del protocollo) Dati personali soggetti a pseudonimizzazione	eCRF / ClinicalOne	Centri/ Sperimentatori (Risoluzion e delle domande)
Dati Revisione medica	La revisione medica dei dati sarà effettuata in collaborazione con lo Sponsor. Dati personali pseudonimizzati del soggetto	Database ospitato in ClinicalOne	Sponsor CRO global (Visualizzazione sull'EDC di dati personali pseudonimizzati del soggetto)

Processo	Descrizione dettagliata del processo	Dati a supporto patrimonio	Destinatario
Analisi statistica	Come da piano di analisi statistica (SAP). dati personali pseudonimizzati del soggetto	Software SAS TFL statistico inviato tramite sistema protetto (Sharepoint)	Sponsor CRO global Statistica Analisi TFL
Trasferimento del database	Database di studio	Tabelle statistiche inviate dal sistema protetto (Piattaforma sFTP)	Sponsor
Rapporto dello studio clinico	Relazione sullo studio clinico redatta secondo le linee guida STROBE Aggregatoe dati personali anonimizzati (date dello studio, dati demografici, dati clinici)	Inviato da sistema protetto (Sharepoint)	Sponsor Autorità regolatorie, quando applicabile

Principi fondamentali

Questa sezione consente di costruire il quadro di conformità per i principi della privacy.

PROPORZIONALITÀ E NECESSITÀ

~~w~~Questa parte consente di dimostrare che sono stati implementati i mezzi necessari per consentire alle persone interessate di esercitare i propri diritti.

Le finalità del trattamento sonospecifiche, esplicite e legittime?

PFM raccoglie i dati esclusivamente per finalità specifiche, esplicite e legittime, al fine di caratterizzare meglio la sicurezza e l'efficacia di tabelecleucel in soggetti con PTLD da EBV+ a seguito di trapianto di cellule ematopoietiche (HCT) o trapianto di organi solidi (SOT).

Quali sono le basi giuridiche che rendono lecito il trattamento?

L'interessato ha dato il proprio consenso al trattamento dei propri dati personali per uno o più scopi specifici nei paesi in cui si applica l'articolo 6.1.a del GDPR, come previsto dalla normativa locale o dalla raccomandazione dell'Autorità locale per la protezione dei dati. Ciò è applicabile a molti Paesi dell'UE, ad eccezione dei casi in cui l'esenzione dal consenso è applicabile in base alla normativa locale per i dati estratti dalla cartella clinica del soggetto.

Per la Francia, la legittimità si basa sull'articolo 6.1.f., il trattamento è necessario ai fini del legittimo interesse perseguito da PFM.

Per l'Italiala liceità del trattamento effettuato dai centripartecipanti, in qualità di titolari del trattamento indipendente, è 'articolo 6. 1. e del Regolamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Per il soggetto vivente, il soggetto ha dato il consenso al trattamento dei propri dati personali per una o più finalità specifiche ai sensi dell'articolo 6.1.a del GDPR.

Data l'impossibilità o lo sforzo sproporzionato di ottenere il consenso dei soggetti per questo studio a causa della natura dello studio che prevede l'inclusione di soggetti deceduti e non più rintracciabili, esiste la possibilità (eccetto che in Italia) di utilizzare l'interesse legittimo come base giuridica (articolo 6.1.f.)

Per tali pazienti (soggetti deceduti o non più rintracciabili o soggetti vivi senza l'impossibilità di ottenere il loro consenso durante il periodo dello studio), i centripartecipanti dovranno documentare nella cartella clinica dei soggetti il motivo dell'impossibilità di ottenere il consenso ed eventualidescrizione dei tentativi fatti per contattare i soggetti e quindi dell'impossibilità di contattarli.

Inoltre, va chiarito che il trattamento dei dati personali in questo studio è necessario per scopi scientifici ai sensi dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o degli Stati membri che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure adeguate e specifiche per salvaguardare i diritti fondamentali e gli interessi dell'interessato, ai sensi dell'articolo 9. 2.j. del Regolamento e ai sensi dell'art. 110 del D.Lgs. 196/2003 in Italia.

I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati ("minimizzazione dei dati")?

La raccolta dei dati personali dei soggetti e degli operatori sanitari è limitata a quanto strettamente necessario per rispondere agli obiettivi dello studio.

Tutte le date (data di iscrizione, data del modulo di consenso, data della lettera informativa, data della diagnosi, date del trattamento, ecc.) vengono registrate secondo il modello GG/MM/AAAA.

Lo stato vitale del soggetto (causa e data del decesso) è necessario per valutare l'efficacia trattamento. Viene utilizzato un elenco a discesa (domande sì/no) e la data viene registrata
nel formato GG/MM/AAAA.

Criteri di eleggibilità richiesti per garantire che il soggetto possa essere incluso nello studio come da regolamento e protocollo (domanda Sì/No).

Le caratteristiche del soggetto (età, sesso, anno di nascita) sono necessarie per caratterizzare la popolazione di soggetti EBV+ PTLD (pediatrici/anziani). Anno di nascita registrato secondo il seguente campo (non viene raccolta la data di nascita completa - AAAA). Genere registrato in base al seguente campo: Maschio / Femmina.

I dati medici raccolti tramite il portale GCT ed estratti dalla cartella clinica serviranno a caratterizzare la popolazione di soggetti EBV+ PTLD e a descrivere il profilo di sicurezza ed efficacia di questi soggetti. Elenco a discesa con risposte pre-identificate, valori di laboratorio, date in GG/MM/AAAA.

I dati sono accurati e aggiornati?

Controlli di qualità dei dati in atto :

Controlli sulla qualità dei dati	Giustificazione
Il monitoraggio dello studio sarà condotto dai monitor delle CRO locali. I monitor dello studio della CRO global effettueranno una verifica continua dei dati di partenza (SDV) per confermare che i dati critici del protocollo (cioè i dati di partenza) inseriti nelle eCRF dal personale autorizzato del sito siano accurati, completi e verificabili dai documenti di partenza.	Un Clinical Research Associate (CRA) della CRO autorizzato ad accedere alle cartelle cliniche si recherà sul posto per effettuare i necessari controlli sui dati e segnalare eventuali deviazioni osservate. Per questo studio viene sviluppato un piano di monitoraggio.
Interrogazioni manuali o automatiche durante tutto il periodo di raccolta dei dati.	Le query sono generate tramite il sistema EDC e possono essere consultate in modo sicuro dal ricercatore principale e dal personale autorizzato a connettersi al sistema. piattaforma.
Conformità dell'EDC a ICH GCP, 21 CFR Part 11 e GDPR requisiti, tra cui la tracciabilità delle registrazioni con la tempistica dell'audit trail	Come parte della conformità di Clinical One.

Qual è la durata di conservazione dei dati?
I dati personali saranno conservati per un periodo coerente con i requisiti normativi relativi alla conduzione dello studio in Europa, compresi gli obblighi di farmacovigilanza (per almeno 15 anni dal termine dello studio.

Principi fondamentali

~~w~~Questa sezione consente di costruire il quadro di conformità per i principi della privacy.

CONTROLLI PER LA TUTELA DEI DIRITTI PERSONALI DEGLI INTERESSATI

~~w~~Questa parte consente di dimostrare che sono stati implementati i mezzi necessari per consentire alle persone interessate di esercitare i propri diritti.

Come vengono informati gli interessati del trattamento?

Il consenso sarà ottenuto da tutti i soggetti (consenso dei genitori per i minori di età o del tutore legale, se nominato), tranne che in Francia, dove non è richiesto dalla normativa locale. I medici partecipanti o il personale autorizzato del centrosaranno responsabili di fornire i documenti informativi ai soggetti e di ottenere (se del caso) il consenso dei soggetti che soddisfano i criteri di inclusione. Il consenso si distinguerà tra il consenso a partecipare allostudio e il consenso al trattamento dei dati personali ai sensi delle normative sulla protezione dei dati in vigore.

Il consenso al trattamento dei dati ~~richiesto per la fornitura del trattamento~~ è distinto dal consenso richiesto per la partecipazione allo studio ~~al PASS~~. Questo consenso deve essere ottenuto prima di avviare un controllo dell'inventario di Tabelecleucel e di ordinare il prodotto.

Il consenso allo studio comprende:

- consenso all'uso secondario dei dati raccolti nel database del portale HCP
- consenso per la raccolta e l'utilizzo dei dati primari

Il formato e il contenuto della lettera informativa per i soggetti e dei documenti di consenso informato saranno conformi ai requisiti degli IRB/IEC, alle leggi e ai regolamenti applicabili del Paese partecipante e descriveranno la natura, lo scopo, le procedure, i rischi e i benefici dello studio. I soggetti saranno inoltre informati del loro diritto di revocareil consenso in qualsiasi momento durante lo studio senza alcuna conseguenza sul precedente trattamento. Il medico partecipante sarà responsabile dell'ottenimento del consenso dei soggetti. Il database conterrà misure di salvaguardia per verificare se il consenso è stato ottenuto. Il modulo di consenso informato sarà fornito al medico partecipante nell'Investigator Site File (ISF) e sarà sottoposto all'Institutional Review Board/Comitato Etico Indipendente se richiesto dalla legislazione locale.

Le procedure di consenso informato per popolazioni specifiche (minori, deceduti e soggetti che hanno perso il follow-up) sono considerate per questo studio e descritte di seguito:

Soggetti minori

Per tutti i soggetti minorenni viventi al momento dell'arruolamento, verrà ottenuto il consenso scritto non opposizioneda parte dei genitori o del tutore legale se nominato.. Inoltre, si otterrà un consenso scritto o una non opposizione per i soggetti minori in grado di acconsentire/assentire legalmente. Il contenuto dei documenti dello studio per i soggetti minorenni inclusi nello studio sarà simile a quello dei documenti per adulti e adattato in base alle fasce d'età specificate dalla normativa locale.

Soggetti deceduti al momento dell'arruolamento

Data la natura dello studio, i soggetti deceduti al momento dell'arruolamento possono essere ammessi allo studio. Per tutti i Paesi partecipanti, le procedure di inclusione dei soggetti deceduti (adulti e minori) devono essere conformi alla normativa locale. Ciò può includere, ad esempio, l'esonero dall'obbligo di raccogliere unconsenso informato, la conferma che il soggetto (quando era in vita) non si è opposto all'uso dei dati sanitariper la ricerca o qualsiasi altro requisito normativo locale, se applicabile.

Soggetti persi al follow-up al momento dell'arruolamento

I centri partecipanti faranno ogni sforzo per contattare e informare i soggetti e lo documenteranno prima di considerare i soggetti persi al follow-up. Le procedure di inclusione dei soggetti persi al follow up, adulti e minori, devono rispettare la normativa locale. Ciò può includere, ad esempio, l'esonero dal consenso informato o qualsiasi altro requisito normativo locale, se applicabile.

Se applicabile, come viene ottenuto il consenso degli interessati?

Il consenso sarà ottenuto da tutti i soggetti (consenso dei genitori per i minori di età o del tutore legale, se nominato, tranne che in Francia, dove non è richiesto dalla normativa locale. I medici partecipanti o il personale autorizzato del centrosaranno responsabili di fornire i documenti informativi ai soggetti e di ottenere (se del caso) il consenso dei soggetti che soddisfano i criteri di inclusione. Il consenso si distinguerà tra il consenso a partecipare allostudio e il consenso al trattamento dei dati personali ai sensi delle normative sulla protezione dei dati in vigore.

In Francia, secondo la normativa locale, non è necessario un consenso informato firmato per arruolare un soggetto in studi non interventistici. Tuttavia, i soggetti devono essere adeguatamente e individualmente informati in conformità alle disposizioni dell'articolo 14 del Regolamento generale sulla protezione dei dati e della Legge francese sulla protezione dei dati (La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés " Loi informatique et Libertés "). In particolare, i soggetti devono essere informati del fatto che possono opporsi alla raccolta dei dati in qualsiasi momento dello studio e senza alcuna conseguenza sulla loro salute.
la loro assistenza continua. I siti partecipanti invieranno la lettera informativa ai soggetti tramite raccomandata con ricevuta di ritorno. L'opposizione alla raccolta dei dati espressa dai soggetti o dai loro rappresentanti in qualsiasi momento dello studio è considerata un ritiro dallo studio.

Per tutti i Paesi, il consenso scritto sarà ottenuto o la lettera informativa sarà inviata prima di qualsiasi trattamento di dati (raccolta di dati secondari tramite trasferimento al portale GCT) o raccolta di dati (raccolta di dati primari tramite cartella clinica).

Come possono gli interessati esercitare i loro diritti di accesso e di portabilità dei dati?

L'interessato può esercitare i propri diritti rivolgendosi prioritariamente al proprio medico curante, anche tramite il Responsabile della protezione dei dati (DPO)del centro, o al DPO dello sponsor.

Portabilità dei dati: i soggetti possono ricevere i propri dati personali in un formato elettronico standardizzato per i Paesi in cui il consenso è la base giuridica (articolo 6.1.a). La portabilità dei dati non è applicabile alla Francia.

Come possono gli interessati esercitare i loro diritti di rettifica e cancellazione?

Diritti di rettifica: Nessun dato personale può essere modificato direttamente dal soggetto nell'e-CRF, ma la modifica dei dati raccolti può essere effettuata se il soggetto ne fa richiesta via e-mail, per posta allo sperimentatore e/o al DPO del sito e/o al DPO dello Sponsor.

Diritto alla cancellazione: il soggetto può esercitare il diritto alla cancellazione dei propri dati personali inviando una richiesta allo sperimentatore e/o al DPO del sito e/o al DPO dello sponsor. La richiesta sarà analizzata dallo sponsor in collaborazione con il Global CRO, in base al tipo di dati che il soggetto desidera cancellare, per valutare il possibile impatto sull'analisi che potrebbe portare a distorsioni e compromettere la ricerca.
A seconda del tipo di dati, alcuni potrebbero essere cancellati, altri no. I soggetti saranno informati se i loro dati possono essere cancellati o meno e il motivo per cui non possono essere cancellati.

Questa valutazione è possibile perché il trattamento è necessario a fini di ricerca scientifica ai sensi dell'articolo 89, paragrafo 1.

Come possono gli interessati esercitare i loro diritti di limitazione e di opposizione?

L'interessato può esercitare i propri diritti rivolgendosi prioritariamente al proprio medico curante, anche tramite la il responsabile della protezione dei dati (DPO) delcentro, o il DPO dello sponsor.

Gli obblighi dei responsabilidel trattamento sono chiaramente identificati e regolati da un contratto?

Il 12 luglio 2023 è stato firmato un contratto di servizio tra PFM e Cerner Enviza France (ora Oracle France SAS), che include le disposizioni contrattuali del GDPR e un accordo sulla sicurezza dei dati, in cui PFM è il Titolare del trattamento dei dati e Oracle France SAS il Responsabile del trattamento dei dati.

In caso di trasferimento di dati al di fuori dell'Unione Europea, i dati sono adeguatamente protetti?

Sì, in base alle Clausole Contrattuali Standard come emanate dalla Commissione Europea (edizione giugno 2021)

I rischi

Questa sezione consente di valutare i rischi per la privacy, tenendo conto dei controlli esistenti o previsti.

La partecipazione allo studio non comporta rischi di natura medica. In particolare, lo studio non comporterà alcuna modifica degli standard di cura dei soggetti, non comprometterà la loro integrità fisica o psicologica e non richiederà visite di controllo speciali per questi soggetti.

Tuttavia, il trattamento dei dati può comportare il rischio di violazione dei diritti e delle libertà dei soggetti. dettagliati nella sezione "VALUTAZIONE DEI RISCHI: POTENZIALI VIOLAZIONI DELLA PRIVACY".

Al fine di ridurre al minimo i rischi derivanti dal trattamento dei dati, PFM e la CRO hanno adottato una serie di misure di sicurezza tecniche e organizzative per proteggere il trattamento dei dati personali nell'ambito dello studio, in conformità con l'articolo 89 del GDPR, e con le disposizioni e le linee guida emanate dalla legge locale sulla privacy, che includono:

Un accordo sulla sicurezza dei dati, parte integrante del contratto di servizi tra PFM e Oracle France SaS, include i controlli di sicurezza e organizzativi.

Il suddettoaccordo sulla sicurezza dei dati comprende i seguenti aspetti:

- Responsabile della sicurezza
- Posizione geografica dei servizi e dei dati
- Ambiente di produzione / non di produzione
- Gestione delle vulnerabilità e delle patch
- Protezione anti-malware
- Politica di backup e ripristino
- Subappalto
- Controllo dell'accesso logico
- Protezione dei dati
- Protezione della comunicazione
- Registri di audit

Misure tecniche adottate dal PFM e/o dalla CRO:

- L'omissione di dati identificativi del paziente (ad es. nome, cognome, data di nascita, ecc.) da qualsiasi rapporto, pubblicazione o altra divulgazione, salvo nei casi previsti dalle leggi vigenti;
- Tecnica di sicurezza per proteggere i dati sensibili: tutti i dati medici/sanitari raccolti saranno pseudonimizzati con un numero unico di identificazione del paziente di 9 cifre (2 cifre per il codice del Paese, 2 per il sito e 5 per il soggetto arruolato). Solo lo sperimentatore o le persone autorizzate che si occupano dello studio all'interno del centro di ricerca hanno la possibilità di accedere ai dati sensibili.
  Solo le persone autorizzate hanno accesso a questo foglio di corrispondenza e alle cartelle cliniche del paziente per tutto il periodo dello studio (CRA per il monitoraggio, autorità competenti). Questo foglio di corrispondenza si trova nella cartella dello studio, che è conservata in un luogo sicuro e chiuso a chiave dell'ospedale ed è accessibile solo al personale sanitario autorizzato a utilizzare la cartella dello studio.
- L'archiviazione dei dati personali dei pazienti, pseudonimizzati, avviene in forma criptata

in formato elettronico, protetto da una password o in una stanza chiusa a chiave presso il centro di ricerca CRO, garantendo che solo il personale espressamente identificato e autorizzato abbia accesso ai dati;

- Il recupero dei dati personali trattati in caso di catastrofe o di qualsiasi altro evento che possa essere qualificato come violazione dei dati.
- In caso di potenziale o effettiva violazione dei dati, la CRO sarà responsabile di determinare se si è effettivamente verificata una violazione dei dati e, in tal caso, di notificare a PFM l'evento, fornendo tutte le informazioni necessarie per consentire a PFM di effettuare le notifiche previste dagli articoli 33 e 34 del GDPR, ove necessario;
- La rimozione dei dati identificativi e/o di qualsiasi altro dato che identifichi e/o renda identificabili i Pazienti e la successiva sostituzione di tali dati con un codice numerico univoco e specifico, al fine di tutelare i diritti degli Interessati quando i dati relativi allo Studio vengono comunicati ad altri soggetti autorizzati;
- Al termine del periodo di conservazione dei dati, PFM adottale tecniche di de-identificazione e anonimizzazione previste dalle linee guida in materia di "De-identification and Anonymization of Individual Patient Data in Clinical Studies";
- l'adozione di adeguate garanzie per il trasferimento dei dati, anche al di fuori del SEE, che consentirà alla PFM di mantenere elevati standard di riservatezza e protezione dei dati personali dei Pazienti in conformità agli articoli 44 e seguenti del GDPR.

Oltre a quanto sopra, Oracle ha adottato misure tecniche e organizzative (TOM) e politiche specifiche che sono:

Politica di protezione dei dati: Pratiche di sicurezza aziendale Oracle settembre 2023 v3.2 (**Appendice 1**)

Oracle dispone di un sistema di allerta per la notifica di violazioni di dati personali e incidenti di sicurezza: "information security incident response", pagina 8 delle "Oracle Corporate Security Practices September 2023 v3.2". Inoltre, è in atto un processo CHIA (Complaint, Hazard, Incident, Accident) che copre la gestione degli incidenti e delle violazioni dei dati. Tutti gli eventi vengono registrati nel software JIRA per tenere traccia dei risultati.

Oracle® Life Sciences Clinical One Cloud Service (Clinical One) soddisfa tutti i criteri di conformità ai requisiti normativi FDA 21 CFR Part 11 ICH GCP descritti nel *documento OLS. C1_Regulatory_Compliance_Addendum_V6_FINAL* (**Appendice 2a**), e sono in atto controlli tecnici, organizzativi e procedurali per soddisfare i requisiti del GDPR (**Appendice 2b**). I dati ospitati e acquisiti da Clinical One si trovano in Germania.

MISURE PREVISTE O ESISTENTI

Questa sezione consente di identificare i controlli (esistenti o pianificati) che contribuiscono alla sicurezza dei dati.

Controlli ambientali e di raffreddamento

· La temperatura e l'umidità ambientale sono mantenute secondo gli standard ASHRAE 9.9.
· Sistema di raffreddamento ridondante (N+1); comprende sistemi ad espansione diretta con condensatori raffreddati ad aria e stazioni centrali con refrigeratori raffreddati ad acqua per il raffreddamento dell'area di calcolo.
· I rilevatori d'acqua sono posizionati nello spazio sotto il pavimento, dove possibile.
· L'umidità è monitorata in tutto lo spazio del data center di Salesforce

Politiche di controllo degli accessi fisici

· Le richieste di accesso devono essere approvate da un membro del team Operazioni tecniche e monitorate tramite un sistema di tracciamento interno.
· Tutte le persone devono presentare un documento d'identità con fotografia rilasciato dal governo (ad esempio, la patente di guida) al personale di sicurezza che rilascia tessere di accesso o badge per i visitatori.

· I visitatori devono essere scortati nello spazio dedicato a Salesforce dal personale Salesforce o dalla sicurezza del centro dati.
· Solo i dipendenti autorizzati di Salesforce Technical Operations hanno accesso fisico ai sistemi di produzione. Questo personale deve registrarsi nel sistema di scansione biometrica prima dell'utilizzo.
· Solo il personale autorizzato di Salesforce ha accesso agli spazi dedicati a Salesforce. L'accesso è inoltre limitato in base alla funzione lavorativa
· L'accesso dei dipendenti viene immediatamente revocato in caso di cessazione del rapporto di lavoro o di trasferimento ad altre mansioni.
· L'accesso al Data Center da parte di personale non dipendente (come i fornitori) deve essere programmato in anticipo dalle Operazioni tecniche e deve presentare un documento d'identità valido con foto e firmare un registro all'arrivo.
· Dopo le opportune verifiche, ai non dipendenti, supervisionati dai dipendenti a tempo pieno di Salesforce, può essere concesso l'accesso allo spazio Salesforce per progetti a tempo determinato.
· I registri di accesso vengono conservati per un minimo di 90 giorni.
· Salesforce Technical Operations esamina i record di accesso (registri ed elenchi di accesso autorizzati) con cadenza trimestrale.

Procedure di controllo degli accessi fisici

· Le lobby dei Data Center sono dotate di personale di sicurezza fisica dedicato in loco 24 ore su 24, con un ingresso a trappola per uomini.
· Il percorso dall'ingresso del data center all'accesso ai server fisici richiede molteplici sfide di sicurezza, tra cui una combinazione di scansioni biometriche a due fattori
· Per ogni tentativo fallito viene registrato un avviso di sicurezza.
· Gli utenti bloccati devono notificare il guasto alla Sicurezza per poter riavere l'accesso.
· I sistemi di produzione Salesforce sono ospitati in uno spazio dedicato e sicuro, separato dal resto del Data Center, che richiede la scansione biometrica e l'accesso tramite badge o pin pad.
· I dipendenti e i fornitori di Salesforce devono restituire i badge di accesso alla sicurezza del centro dati al momento della partenza.
· Tutte le persone sono soggette a perquisizione all'ingresso e prima di lasciare la struttura Salesforce utilizza centri dati colocalizzati per ospitare il nostro ambiente di produzione. Salesforce gestisce un centro dati primario e un centro dati di failover per ogni istanza del nostro servizio, in caso di guasto catastrofico del centro dati primario. Esistono altre strutture utilizzate come ambienti/laboratori di prova. Solo i dipendenti autorizzati di Salesforce Technical Operations hanno accesso a queste strutture.
· I sistemi Salesforce che forniscono la soluzione sono contenuti in uno spazio dedicato e sicuro, separato dal resto del Data Center. Le gabbie all'interno della stanza si estendono fino ai passacavi sopraelevati. I sensori di movimento e le telecamere posizionate a questo livello rilevano qualsiasi movimento e attivano gli avvisi per la sorveglianza della sicurezza.
Controlli aggiuntivi della struttura
· Sono previsti controlli di accesso limitati per proteggere l'ingresso alla postazione Meet-Me, un'area segregata per le connessioni esterne tra i sistemi Salesforce e i circuiti del carrier. L'accesso a questo spazio è limitato al personale del centro dati di co-locazione.
· Tutti i punti di ingresso (ad esempio, tetto, tombini,celle di servizio e di rete, porte) sono monitorati.
· Videosorveglianza interna ed esterna con sensori di movimento nelle aree chiave per rilevare le attività. I video vengono archiviati su disco e conservati per un minimo di tre (3) mesi.
· Pattuglie di sicurezza di terzi in tutta la struttura e nei terreni esterni
· L'area di spedizione/ricezione è fisicamente isolata dall'area di elaborazione. L'area di spedizione/ricevimento è monitorata tramite video, l'accesso al piano del data center è limitato e gestito dal personale del data center di co-locazione.
· Nelle aree protette è vietato l'uso di dispositivi fotografici, video, audio e altri dispositivi di registrazione mobile.
a meno che non sia autorizzato

Manutenzione dei sistemi di raffreddamento

· I sistemi di raffreddamento sono mantenuti e testati secondo le raccomandazioni del produttore (OEM).
· Edificio progettato per i rischi locali di sismicità, tempesta e alluvione
· Situato sopra il livello del mare senza scantinato e con un sistema di drenaggio/evacuazione

Potenza

· Alimentazione elettrica sotterranea. Tutti gli interruttori elettrici si trovano all'interno dell'edificio e queste aree sono accessibili solo al personale autorizzato del data center.
· Le sale comunicazioni e server hanno due fonti di alimentazione indipendenti.
· Generatori ridondanti (N+1)
· Unità di distribuzione dell'alimentazione (PDU) ridondanti
· Sistemi UPS ridondanti (N+1)
· Lo stoccaggio del carburante in loco garantisce un'autonomia minima di 24 ore a pieno carico in caso di disastro.
· I centri dati mantengono contratti con più fornitori di rifornimento.

Replica dei dati

In Salesforce, la fiducia è il nostro valore# 1 e la nostra strategia di data center supporta l'impegno dell'azienda a gestire il servizio di cloud computing più sicuro, affidabile e disponibile. Il successo dei clienti è alla base della nostra strategia per i data center e offrire i più alti standard di disponibilità, prestazioni e sicurezza è la nostra massima priorità. A tal fine, costruiamo e serviamo ogni istanza di Salesforce da due data center geograficamente diversi per evitare singoli punti di guasto nella nostra infrastruttura. Questo progetto supporta la disponibilità continua che i nostri clienti si aspettano da noi.

In qualsiasi momento, la vostra istanza Salesforce viene servita attivamente da una sede con transazioni replicate quasi in tempo reale in una sede secondaria completamente ridondante. Effettuiamo regolarmente il passaggio da una sede all'altra per motivi di manutenzione, conformità e disaster recovery. Poiché continuiamo a espandere e migliorare la nostra presenza infrastrutturale globale, consigliamo ai clienti di costruire le loro applicazioni senza requisiti specifici di data center per supportare un'esperienza Salesforce senza soluzione di continuità.

Inoltre, disponiamo di istanze servite dall'infrastruttura cloud di Amazon Web Services (AWS) negli Stati Uniti, in Canada, in India e in Australia. Queste istanze sono situate in due o più zone di disponibilità separate all'interno di ciascun Paese.

Per informazioni su come determinare l'ubicazione dell'istanza, consultare questo articolo di conoscenza: https://help.salesforce.com/articleView?id=Where-is-my-Salesforce-instance-located&type=1&mode=1

Manutenzione dei sistemi

· I centri di elaborazione dati ubicati testano e mantengono i loro sistemi di alimentazione in base agli standard del settore, come minimo. Rete
· Volte in cemento per l'ingresso della fibra
· Percorsi interni ridondanti
· Neutrale rispetto alla rete; si collega ai principali vettori

Soppressione incendi

· I sensori VESDA (Very Early Smoke Detection Apparatus) sono installati in tutto il data center e nei punti di campionamento dei sistemi di trattamento dell'aria.
· La soppressione degli incendi ad acqua con tubi a secco a doppio allarme ‡doppio blocco, multizona, limita l'intervento solo alle aree interessate
· I rilevatori di fumo sono distribuiti a livello del soffitto e sotto il pavimento rialzato in tutte le strutture del centro dati co-locate.
· Tutti i sistemi di soppressione degli incendi sono ispezionati internamente dal personale del centro dati di colocazione o dal personale OEM secondo le raccomandazioni del produttore.
·

· Gli estintori ad azionamento manuale sono presenti in tutta la struttura e vengono ispezionati in base agli standard OEM e con cadenza almeno annuale Monitoraggio Il personale tecnico del centro dati provvede al monitoraggio 24 ore su 24 nella sala operativa.
· Il personale del centro dati è in grado di monitorare a distanza tutti i sistemi ambientali del centro dati. Piano d'azione per le emergenze Ciascun centro dati colocalizzato dispone di un piano d'azione per le emergenze documentato.
· I dipendenti del centro dati sono addestrati all'esecuzione del piano.
· Il piano include le informazioni di contatto per i servizi di emergenza locali

Politiche di accesso fisico

Salesforce mantiene un sistema formale di gestione della sicurezza delle informazioni (ISMS) a livello aziendale, conforme ai requisiti della norma ISO 27001, che comprende politiche, standard e procedure di sicurezza. Politiche, procedure e descrizioni delle mansioni formali sono documentate per le aree operative, tra cui: operazioni del centro dati, viluppo, gestione dei programmi gestione della produzione ingegneria delle infrastrutture, ingegneria della qualità, gestione delle release operazioni, assunzioni e cessazioni. Queste politiche e procedure sono state sviluppate per separare le mansioni e applicare le responsabilità in base alla funzionalità del lavoro.

Accesso fisico Comunicazione

Salesforce verifica tutti gli accessi degli utenti ai sistemi, alle applicazioni e ai database almeno ogni 90 giorni. L'accesso degli appaltatori viene rivisto 90 giorni dopo il provisioning e richiede una nuova approvazione da parte del manager che lo ha approvato per continuare o terminare l'accesso.

Manutenzione dell'hardware

Salesforce affitta la maggior parte dell'hardware per un periodo di tre anni, quindi il refresh dell'hardware avviene almeno una volta ogni tre anni. Tuttavia, poiché Salesforce trae enormi vantaggi dai progressi tecnologici grazie alla sua architettura multi-tenant, spesso effettua aggiornamenti dell'hardware con un ciclo più breve.

Piano di continuazione dell'attività

Salesforce ha sviluppato un programma globale di Business Continuity e Disaster Recovery per i servizi Salesforce; ha assunto pianificatori certificati di Business Continuity (CBCP) e si è avvalsa dei servizi di consulenti leader per assistere nello sviluppo continuo di piani e procedure di Business Continuity e Disaster Recovery. Questo programma è supervisionato dal senior management di ciascuna delle principali aree funzionali di Salesforce ed èsupportato dalla leadership esecutiva ai massimi livelli

Salesforce dispone di un Crisis Management Team (CMT) composto da dirigenti selezionati dei reparti chiave a livello globale. Il CMT viene mobilitato quando si verifica una crisi o un evento significativo ed è responsabile di valutare la situazione e di rispondere di conseguenza. A seconda della gravità e della natura dell'incidente, il leader della CMT può richiedere l'impegno di vari team di supporto per contribuire alla mitigazione dell'incidente. La CMT si riunisce periodicamente per la formazione, l'addestramento e la revisione della Guida all'azione della CMT documentata, oppure quando è necessario a causa di una crisi o di un evento significativo. I membri della CMT hanno ruoli e responsabilità specifici e devono essere sempre disponibili (24/7/365). La CMT conduce esercitazioni da tavolo, almeno una volta all'anno.

Salesforce gestisce un Mirror Site che è un sito caldo al 100% con replica dei dati in tempo reale (async). Il data center secondario è replicato al 100% della capacità (host, rete e storage) del data center di produzione. Nell'ambito dello sviluppo di un piano e di un programma di Disaster Recovery validi, Salesforce pianifica esercitazioni di Disaster Recovery che vengono condotte più volte all'anno. Salesforce testerà il suo piano di disaster recovery almeno su base annuale e continuerà a migliorare e sviluppare i processi e la tecnologia relativi aldisaster recovery per ridurre ulteriormente gli RPO e gli RTO. Salesforce ha sviluppato ulteriori procedure, processi e piani, tra cui un piano contro le pandemie.

Inoltre, i processi di comunicazione in caso di catastrofe vengono esercitati utilizzando il sistema di notifica di massa durante ogni esercitazione, che comprende chiamate con richieste di risposta al team di gestione delle crisi di Salesforce e ai team di disaster recovery di produzione.

Alimentazione e comunicazione

Per massimizzare la disponibilità, il servizio viene fornito utilizzando più data center di livello mondiale che supportano istanze primarie e replicate di disaster recovery, oltre a una struttura di laboratorio separata di livello produttivo. L'infrastruttura utilizza componenti di classe carrier progettati per supportare milioni di utenti. L'uso estensivo di server e tecnologie di rete ad alta disponibilità e una strategia di rete neutrale rispetto ai carrier contribuiscono a ridurre al minimo il rischio di singoli punti di guasto e a fornire un ambiente altamente resiliente con tempi di attività e prestazioni ottimali. I servizi Salesforce sono configurati per essere ridondanti almeno N+1, dove N è il numero di componenti di un determinato tipo necessari per il funzionamento del servizio e +1 è la ridondanza. In molti casi, Salesforce dispone di più di un'apparecchiatura ridondante per una determinata funzione.

Sicurezza di rete

Come previsto dalla politica di protezione della rete di Salesforce:

- Le reti devono essere segregate, con mezzi logici e/o fisici. Oltre a utilizzare dispositivi fisici separati, le architetture di rete si avvalgono di tecnologie di virtualizzazione della sicurezza per implementare reti virtuali, switch, interfacce e così via. Questi componenti di rete virtuale isolano e proteggono il traffico di rete per soddisfare i requisiti di segregazione di questa sezione.
- L'architettura di rete definisce sottoreti per i componenti del sistema accessibili al pubblico che separano il traffico esterno da quello sulle reti interne di Salesforce.
- Il traffico deve essere controllato e segregato in base alla funzionalità richiesta e alla classificazione dei dati/sistemi in base ai rischi e ai rispettivi requisiti di sicurezza.
- È inoltre richiesta la segregazione tra le funzionalità dell'utente (ad esempio, i servizi Web) e le funzionalità di gestione del sistema informativo (ad esempio, i database).
- A meno che il rischio non sia identificato e accettato dal proprietario dei dati, i sistemi sensibili devono essereisolati (fisicamente o logicamente) dalle applicazioni/sistemi non sensibili.

- Controlli di sicurezza specifici per la zona e per il centro dati di prima parte
- Tutte le zone collegate a reti non attendibili (ad esempio, Internet, ISP) devono utilizzare un router edge/border per la terminazione dei collegamenti.
- Per limitare il traffico, tra i router edge/di confine e i router interni del data center devono essere installate delle ACL o un altro meccanismo di sicurezza forte.
- I router di confine dovrebbero essere utilizzati solo per interfacciarsi con gli ISP e altri fornitori di transito.

Rete condivisa

Salesforce ha implementato un approccio di segmentazione della rete a zone, con firewall e sistemi di rilevamento delle intrusioni opportunamente posizionati all'interno di ciascuna zona. I firewall esterni consentono solo il traffico http e https sulle porte 80 e 443, oltre al traffico ICMP. Gli switch garantiscono la conformità della rete allo standard RFC 1918 e le tecnologie di traduzione degli indirizzi migliorano ulteriormente la sicurezza della rete. Il traffico in ingresso attraversa un livello edge e un livello di bilanciamento del carico prima di incontrare il livello di inoltro del datacenter, che instrada le richieste secondo le necessità.

Le politiche di gestione della rete di Salesforce definiscono meccanismi di protezione che includono:

- Le connessioni di rete esterne vengono instradate attraverso meccanismi di protezione dei confini.
- I diagrammi della topologia di rete sono progettati in modo da determinare se esistono meccanismi di protezione dei confini per gestire le connessioni esterne in entrata e in uscita.
- Gli standard di sicurezza di rete di Salesforce definiscono i requisiti per l'instradamento del traffico esterno attraverso meccanismi di protezione dei confini.

· L'ispezione degli elenchi di controllo degli accessi (ACL) o delle regole del firewall su una selezione di dispositivi di rete viene utilizzata per determinare se il traffico esterno è stato instradato in conformità allo standard di sicurezza della rete di produzione di Salesforce.
· Le porte e i protocolli di rete approvati sono implementati in conformità agli standard di rete di produzione documentati.

Gestione delle vulnerabilità e patch

Salesforce ha adottato una politica che prevede l'esecuzione di scansioni periodiche delle vulnerabilità su tutti i sistemi informativi e le applicazioni ospitate di Salesforce. La frequenza e la completezza delle scansioni sono definite in base alla categorizzazione di sicurezza del sistema, alla sensibilità dei dati e/o a specifici requisiti normativi. Molte di queste scansioni vengono eseguite almeno mensilmente su tutti i prodotti Salesforce. Vengono utilizzati meccanismi automatizzati per confrontare i risultati delle scansioni di vulnerabilità nel tempo e determinare le tendenze delle vulnerabilità del sistema informativo.

I rapporti di scansione delle vulnerabilità e i risultati delle valutazioni dei controlli di sicurezza vengono analizzati e, quando nuove vulnerabilità possono interessare il sistema/applicazione, vengono identificate e segnalate.

· Gli strumenti e le tecniche di scansione delle vulnerabilità che facilitano l'interoperabilità tra gli strumenti e l'automazione di parti del processo di gestione delle vulnerabilità devono essere distribuiti utilizzando gli standard per:
· Enumerazione di piattaforme, difetti del software e configurazioni improprie;
· Formattazione di liste di controllo e procedure di test; e

· Misurare l'impatto della vulnerabilità.

Le vulnerabilità identificate vengono assegnate in base alla priorità con un accordo di livello di servizio interno associato per la correzione in base al rischio. La direzione di Salesforce esamina lo stato delle vulnerabilità e delle patch con cadenza bisettimanale. Le patch vengono distribuite per le vulnerabilità note almeno mensilmente o in base alla necessità in base alla criticità.

Controllo di virus e malware

Salesforce ha implementato il rilevamento di malware a livello di rete nell'ambiente di produzione. In particolare, i sistemi di rilevamento delle intrusioni di rete sono configurati (e continuamente aggiornati) per rilevare il traffico di rete legato al malware. Vengono utilizzati anche altri controlli per affrontare le minacce informatiche, come l'indurimento del sistema operativo dei nostri server basati su UNIX e Linux e la configurazione del firewall per garantire che vengano aperte solo le porte necessarie e negate tutte le altre. L'accesso a questi sistemi è limitato al personale autorizzato e tutti questi sistemi, così come le piattaforme host, sono monitorati in tempo reale attraverso un sistema di monitoraggio della sicurezza. Salesforce non limita i tipi di file che gli utenti possono caricare. Salesforce non analizza, modifica o pulisce i dati dei clienti; il sistema memorizza le informazioni fornite in un formato codificato all'interno del database. Si consiglia ai clienti di utilizzare soluzioni antivirus e antimalware aggiornate per ridurre queste minacce. Il sistema di produzione riceve posta in entrata come parte della funzionalità del flusso di lavoro, ma poiché l'architettura del sistema non consente l'esecuzione o il trasferimento del codice nelle e-mail, ciò non rappresenta una minaccia per la nostra rete, applicazione o utenti. Le e-mail inviate dall'applicazione Salesforce non sono attualmente sottoposte a scansione per la ricerca di virus. I clienti possono implementare prodotti partner come WithSecure (noto anche come F-Secure) Cloud Protection for Salesforce per fornire una sicurezza aggiuntiva contro le minacce informatiche per i contenuti caricati.

Per ulteriori informazioni, consultare l'articolo di H&T qui (sezione sul caricamento dei file) - https://help.salesforce.com/s/articleView?id=000318378&type=1# FileUpload

Salesforce impone l'installazione di software anti-malware sulle workstation dei dipendenti e sui server aziendali. I server genitori delle definizioni di malware controllano quotidianamente gli aggiornamenti e li inviano alle workstation e ai server degli utenti finali, che sono configurati in modo da impedire agli utenti finali di disabilitare in modo permanente la scansione antimalware. Vengono generati avvisi in caso di compromissione o potenziale compromissione. L'accesso privilegiato al server antimalware gestito è limitato agli amministratori di sistema.

Segmentazione della piattaforma di allestimento/produzione

Esiste un numero limitato di dipendenti di Salesforce Technical Operations con accesso logico ai sistemi. Questi utenti privilegiati devono autenticarsi al sistema gateway Production Remote Access (PRA). Il sistema PRA ospita un ambiente sicuro in cui gli utenti privilegiati gestiscono i sistemi di produzione, ricevendo solo una rappresentazione bitmap di uno schermo virtuale ospitato nell'ambiente sicuro. Gli utenti con accesso privilegiato devono autenticarsi a un server sicuro utilizzando due livelli di autenticazione a due fattori.

I controlli aggiuntivi includono:

- Le applicazioni di gestione non vengono eseguite localmente sulle postazioni di lavoro.
- Gli utenti non possono copiare-incollare i dati dall'ambiente ospitato.
- Gli utenti possono avviare solo due applicazioni pre-approvate: un browser Web (con accesso limitato a Internet) e un terminale.
- SSH è consentito solo attraverso gli host bastion.
- Le connessioni a Internet dal client sono consentite solo tramite proxy autenticati e registrati.
- Sono vietati i servizi di messaggistica istantanea, e-mail/webmail e qualsiasi altro servizio fornito da Corp IT.
- Gli account amministrativi sono gestiti centralmente, tramite TACACS+/Kerberos e un sistema di autenticazione a due fattori.
- Gli utenti privilegiati devono accedere utilizzando ID utente univoci.
- Gli account generici/condivisi sono accessibili solo tramite sudo e questi eventi vengono registrati a livello centrale.

Amministrazione dell'accesso:

Le Operazioni tecniche approvano il login e l'accesso alla rete per i server e le altre apparecchiature dell'infrastruttura. Gli account amministrativi vengono bloccati automaticamente dopo 90 giorni di inattività e richiedono il ripristino della password da parte di un amministratore. Al termine, gli account privilegiati vengono bloccati in Kerberos, le connessioni vengono interrotte e i token vengono rimossi. Anche le connessioni VPN/jumphost in sospeso vengono interrotte. Se un utente viene trasferito ma mantiene un accesso non privilegiato, i privilegi amministrativi vengono revocati a livello centrale. Le attività di cessazione vengono attivate automaticamente su notifica delle Risorse Umane. L'accesso logico viene rivisto trimestralmente dalla direzione delle operazioni tecniche.

Controllo delle modifiche

Salesforce: Una procedura formale di gestione delle patch fa parte del processo di gestione delle modifiche di Salesforce ed è finalizzata a massimizzare il tempo di attività e a ridurre al minimo i tempi di inattività del servizio, confermando che le modifiche relative ad aggiornamenti, patch e correzioni di sicurezza rilasciate dai fornitori sono formalmente documentate e valutate.
Il processo di gestione delle modifiche richiede che le richieste di modifica siano registrate, valutate, autorizzate, classificate per priorità, pianificate, testate, implementate, documentate e riviste in modo controllato. Gli amministratori di sistema valutano le modifiche per determinare la criticità per l'ambiente di produzione.

Modis: Nel nostro processo definito, sono disponibili diversi ambienti e uno strumento di ticketing è impostato per fare riferimento a tutte le funzionalità e le modifiche. Ogni parte della documentazione viene aggiornata in base alle informazioni disponibili nel nostro strumento. Inoltre, un ambiente (INT) viene utilizzato dal team Modis per convalidare gli sviluppi. Il secondo ambiente (Recette/UAT) è utilizzato dai team di Modis e Pierre Fabre per testare e convalidare le implementazioni. Una volta terminata questa fase di test, i team di Pierre Fabre danno il "via" formale per passare alla produzione. Tutti i componenti del progetto sono archiviati in un repository per garantire il controllo delle fonti. Ciascuna attività manuale è inoltre referenziata in un file separato e ogni attività viene eseguita al momento della distribuzione.

Crittografia

Le informazioni archiviate all'interno dell'infrastruttura di database multi-tenant e di archiviazione dei documenti sono crittografate a riposo all'interno del file system.

Salesforce è consapevole del fatto che la scelta di archiviare dati sensibili, confidenziali o proprietari presso una terza parte spesso spinge i clienti a esaminare più da vicino le politiche di conformità dei dati sia esterne che interne. Quando i clienti guardano a normative come PCI-DSS, HIPAA/HITECH e FedRAMP attraverso la lente dell'adozione di servizi basati sul cloud, di solito adottano un approccio pragmatico ma conservativo alla protezione dei dati nel cloud. Per facilitare i requisiti più avanzati di crittografia dei dati a riposo, Salesforce offre Shield Platform Encryption, che offre ai clienti la possibilità di fornire le proprie chiavi, oltre a funzioni di gestione del ciclo di vita delle chiavi di crittografia. Shield Platform Encryption è disponibile come abbonamento aggiuntivo per le edizioni Enterprise, Performance e Unlimited. Per ulteriori informazioni, consultare la documentazione del prodotto: https://help.salesforce.com/articleView?id=sf.security_pe_overview.htm&type=5.

Trasferimento protetto dei dati

Tutte le trasmissioni tra l'utente e i Servizi Salesforce sono protette mediante TLS 1.2 e crittografate con chiavi a 256 o 128 bit. I servizi utilizzano certificati SSL di impostazione internazionale/globale con chiavi pubbliche a 2048 bit. L'elenco delle suite di cifratura supportate è disponibile nella knowledge base di Salesforce: https://help.salesforce.com/articleView?id=000351980&language=de&mode=1&type=1.

Gestione dei dati protetta

Salesforce funziona su un'architettura multi-tenant e i dati sono logicamente segregati. Questa è una spiegazione di alto livello del processo di autenticazione e del modo in cui i dati sono segregati tra le organizzazioni (ad esempio i clienti).

-Un utente si collega a login.salesforce.com e accede al nostro servizio inserendo le proprie credenziali (nome utente e password). Salesforce emette quindi un token di sessione sicuro per l'utente, che viene inviato avanti e indietro dal server di Salesforce. con ogni richiesta fatta al nostro servizio. Questo token di sessione viene mappato in quello che chiamiamo "contesto utente" all'interno dei servizi Salesforce. Il contesto dell'utente include l'organizzazione a cui l'utente appartiene e chi è l'utente all'interno dell'organizzazione.

L'organizzazione a cui l'utente appartiene è il modo in cui i dati vengono codificati all'interno delle tabelle di Oracle, quindi ogni record di ogni tabella ha un ID organizzazione Char 15 codificato Base62. Ogni query creata dal nostro servizio include una "clausola where", che comprende l'ID organizzazione e l'ID utente: ID organizzazione e ID utente. L'ID dell'organizzazione separa i dati dell'utente da quelli di altre organizzazioni, mentre l'ID dell'utente definisce il modello di condivisione di ciò che l'utente potrà visualizzare all'interno dello spazio dell'organizzazione. Per ogni pagina visualizzata, il servizio conferma che la sessione è valida confrontando il token di sessione inviato dal client con il token presente nella tabella dello stato della sessione.

Se il token di sessione non corrisponde, il servizio disconnette automaticamente l'utente. Gli script dell'applicazione aggiungono automaticamente alla query SQL l'ID dell'organizzazione e l'ID dell'utente nella clausola where della query, recuperano le righe, convalidano che le righe corrispondano ancora alla sessione che le ha richieste, eliminano l'ID dell'organizzazione e l'ID dell'utente, creano dichiarazioni di stampa e inviano i dati richiesti al browser e la pagina con i dati richiesti viene resa.

Protezione dei dati

Le terze parti incaricate da Salesforce sono tenute a sottoscrivere accordi di riservatezza sui dati dei clienti. Tutte le terze parti sono soggette alle politiche e alle procedure di Salesforce, come definito nello standard aziendale sui fornitori di terze parti e in altre politiche. Ciò include elementi quali lo screening dei precedenti, la formazione e la violazione delle policy e l'applicazione delle stesse. I potenziali fornitori che supportano l'ambiente di produzione dei servizi Salesforce vengono valutati per quanto riguarda la sicurezza, la conformità e le pratiche di privacy prima di firmare i contratti per i servizi. Anche questi fornitori terzi vengono valutati dal team di conformità di Salesforce prima del go-live. Le carenze riscontrate nella revisione vengono corrette e/o vengono identificati controlli compensativi per affrontare i rischi principali, prima dell'avvio dell'attività con potenziale accesso ai dati dei clienti. Sono stati stipulati contratti con tutte le terze parti che supportano l'ambiente di produzione e questi fornitori terzi sono controllati in base agli SLA e ai termini del loro contratto, compresa l'adesione alle politiche e alle procedure di Salesforce e alle pratiche di sicurezza fisica e delle informazioni, almeno su base annuale.

Impegno di terzi

Le terze parti incaricate da Salesforce sono tenute a sottoscrivere accordi di riservatezza sui dati dei clienti. Tutte le terze parti sono soggette alle politiche e alle procedure di Salesforce, come definito nello standard aziendale sui fornitori di terze parti e in altre politiche. Ciò include elementi quali lo screening dei precedenti, la formazione e la violazione delle policy e l'applicazione delle stesse. I potenziali fornitori che supportano l'ambiente di produzione dei servizi Salesforce vengono valutati per quanto riguarda la sicurezza, la conformità e le pratiche di privacy prima di firmare i contratti per i servizi. Anche questi fornitori terzi vengono valutati dal team di conformità di Salesforce prima del go-live. Le carenze riscontrate nella revisione vengono corrette e/o vengono identificati controlli compensativi per affrontare i rischi principali, prima dell'avvio dell'attività con potenziale accesso ai dati dei clienti. Sono stati stipulati contratti con tutte le terze parti che supportano l'ambiente di produzione e questi fornitori terzi sono controllati in base agli SLA e ai termini del loro contratto, compresa l'adesione alle politiche e alle procedure di Salesforce e alle pratiche di sicurezza fisica e delle informazioni, almeno su base annuale.

Indietro

I supporti di backup sono crittografati con un modulo di crittografia conforme a FIPS 140-2 che utilizza AES256. I backup non lasciano fisicamente i centri dati Salesforce e l'accesso è limitato al personale autorizzato. I backup sono conservati in uno spazio sicuro e dedicato del nostro centro dati fino a quando non devono essere ritirati e distrutti.

I dati dei clienti attivi rimangono in memoria finché il cliente non li cancella o li modifica. I dati eliminati dal cliente sono temporaneamente disponibili nel Cestino dell'applicazione per 15 giorni, dopodiché i record vengono contrassegnati per l'eliminazione e non sono più disponibili per gli utenti. I dati contrassegnati per l'eliminazione vengono eliminati in modo permanente dai processi batch per un periodo di 90 giorni dopo la marcatura per l'eliminazione. Sia i dati del cliente che quelli contrassegnati per l'eliminazione vengono conservati su supporti di backup per 90 giorni (30 giorni per le istanze sandbox).

Registro di controllo

I registri dell'infrastruttura interna di Salesforce vengono raccolti da vari strumenti di monitoraggio per le attività sui sistemi che ospitano Salesforce e comprendono:

- Accesso al server
- Accesso alla rete
- Eventi di gestione del firewall
- Traffico dei sistemi di rilevamento delle intrusioni di rete (basato su firme e anomalie)
- Database
- Integrità dei file
- Configurazione del dispositivo di rete

Gli eventi di registro vengono correlati per generare avvisi. Gli avvisi sono configurati per notificare i team Technical Operations e Computer Security Incident Response Team (CSIRT). Gli avvisi di sicurezza devono essere confermati e seguiti, se opportuno, dal CSIRT. I firewall e i sistemi IDS sono configurati con notifiche syslog automatiche per gli eventi chiave. I registri vengono archiviati e attualmente sono conservati per un minimo di (1) un anno. I registri dell'infrastruttura vengono eliminati dai dati personali che fanno parte dei dati del cliente prima di essere archiviati nell'infrastruttura di registrazione centrale.

I log dell'infrastruttura vengono raccolti e archiviati in un sistema di gestione dei log gestito dall'organizzazione Salesforce Security. Gli utenti di questo sistema non hanno la possibilità di modificare o eliminare i dati dei registri. L'accesso amministrativo a questo ambiente è limitato a un numero ristretto di persone autorizzate all'interno dell'organizzazione di sicurezza.

Revisione dei registri

I log dell'infrastruttura vengono raccolti e archiviati in un sistema di gestione dei log gestito dall'organizzazione Salesforce Security. Gli utenti di questo sistema non hanno la possibilità di modificare o eliminare i dati dei registri. L'accesso amministrativo a questo ambiente è limitato a un numero ristretto di persone autorizzate all'interno dell'organizzazione di sicurezza. Il Computer Security Incident Response Team (CSIRT) di Salesforce utilizza un sistema di registrazione e gestione degli eventi di sicurezza per gestire gli avvisi e i registri di sicurezza generati dai dispositivi della nostra rete. Il sistema consiste in un database centrale, un server di gestione e agenti distribuiti. Gli agenti distribuiti ricevono eventi da dispositivi e sistemi di rete (firewall, IDS, router, switch, host, integrità dei file e monitoraggio dei database) sulla rete, comprimono,criptano e trasmettono i dati al server di gestione e al database per l'elaborazione. Gli eventi correlati sono configurati in modo da generare avvisi e registri che vengono monitorati 24 ore su 24, 7 giorni su 7.
I firewall e i sistemi IDS sono configurati con notifiche syslog automatiche per gli eventi chiave. I registri vengono archiviati e attualmente sono conservati per un minimo di 1 anno.

Comunicazione criptata

Tutte le trasmissioni tra l'utente e i Servizi Salesforce sono protette mediante TLS 1.2 e crittografate con chiavi a 256 o 128 bit. I servizi utilizzano certificati SSL di impostazione internazionale/globale con chiavi pubbliche a 2048 bit. L'elenco delle suite di cifratura supportate è disponibile nella knowledge base di Salesforce:
https://help.salesforce.com/articleView?id=000351980&language=de&mode=1&type=1.

Autenticazione degli utenti

Salesforce offre diversi metodi per autenticare gli utenti. Alcuni metodi sono abilitati automaticamente, mentre altri richiedono l'abilitazione e la configurazione da parte dell'utente.
Per l'autenticazione degli utenti è possibile utilizzare il single sign-on e l'autenticazione a due fattori. Salesforce dispone di un proprio sistema di autenticazione degli utenti, ma alcune aziende preferiscono utilizzare una funzionalità di single sign-on esistente per semplificare e standardizzare l'autenticazione degli utenti. Esistono due opzioni per implementare il single sign-on: l'autenticazione federata tramite Security Assertion Markup Language (SAML) o l'autenticazione delegata. L'autenticazione federata tramite Security Assertion Markup Language (SAML) consente di inviare dati di autenticazione e autorizzazione tra servizi Web affiliati ma non correlati. Ciò consente di accedere a Salesforce da un'applicazione client. L'autenticazione federata con SAML è abilitata per impostazione predefinita per l'organizzazione. L'autenticazione delegata single sign-on consente di integrare Salesforce con un metodo di autenticazione scelto dall'utente. Ciò consente di integrare l'autenticazione con il server LDAP (Lightweight Directory Access Protocol) o di eseguire il single sign-on autenticandosi con un token anziché con una password. È possibile gestire l'autenticazione delegata a livello di autorizzazioni, consentendo ad alcuni utenti di utilizzare l'autenticazione delegata, mentre altri utenti continuano a utilizzare la propria password gestita da Salesforce. L'autenticazione delegata è impostata dalle autorizzazioni, non da organizzazione. I motivi principali per utilizzare l'autenticazione delegata sono: - Utilizzare un tipo di autenticazione utente più forte, come l'integrazione con un provider di identità sicure - Rendere la pagina di accesso privata e accessibile solo dietro un firewall aziendale - Differenziare l'organizzazione da tutte le altre aziende che utilizzano Salesforce per ridurre gli attacchi di phishing È necessario richiedere l'abilitazione di questa funzione a Salesforce. Contattate Salesforce per abilitare l'autenticazione delegata single sign-on per la vostra organizzazione. I fornitori di autenticazione consentono agli utenti di accedere all'organizzazione Salesforce utilizzando le credenziali di accesso di un fornitore di servizi esterno.

Salesforce supporta il protocollo OpenId Connect che consente agli utenti di accedere da qualsiasi provider OpenID come Google, PayPal, LinkedIn e altri servizi che supportano OpenID Connect. Quando i provider di autenticazione sono abilitati, Salesforce non convalida la password dell'utente. Al contrario, Salesforce utilizza le credenziali di accesso dell'utente dal fornitore di servizi esterno per stabilire le credenziali di autenticazione. Queste informazioni sono state ricavate dal seguente articolo di Aiuto e formazione: https://help.salesforce.com/HTViewHelpDoc?id=security_overview_auth.htm

VALUTAZIONE DEL RISCHIO: POTENZIALI VIOLAZIONI DELLA PRIVACY

Analisi e valutazione dei rischi

Il rischio	Principali fonti di rischio	Principali minacce	Principali impatti potenziali	Controlli principali che riducono la gravità e la probabilità	Gravità	Probabilità
Accesso illegittimo ai dati	Investigatore Persone non autorizzate	Trattamento dei dati personali senza la consapevolezza del rischio di violazione dei dati. Divulgazione accidentale Cyberattacco Furto di dati	Mancato rispetto dei diritti e delle libertà del soggetto. Ad esempio: sensazione di invasione della privacy con danni irreversibili, sensazione di violazione dei diritti fondamentali (ad esempio, discriminazione, libertà di espressione), cyberbullismo e molestie.	Sensibilizzazione e formazione all'attivazione del centro e durante la fase di svolgimento dello studio attraverso visite di monitoraggio e/o comunicazione No dati identificativi diretti raccolti (cognome, nome, e-mail, indirizzo, ecc.) che possano essere utilizzati per identificare il soggetto. Misure di crittografia per i dati ospitati e archiviati Accesso limitato ai file con una limitazione di durata	Significativo	Limitato

				Misure organizzative (autorizzazione del personale), rapporti con terzi)		
Modifica indesiderata dei dati	Errore umano (dipendente interno) Fallimento inSistema IT	Alterazione accidentale dei dati	Necessità di raccogliere i dati corretti dalle registrazioni dei soggetti (conservate in un luogo sicuro all'interno d e l sito) senza identificare nuovamente il il soggetto	Poiché tutti i dati sono archiviati nel database clinico con provedi audit, i controlli di modifica e le query manuali sono sollevati dal monitoraggio, dalla gestione dei dati, dalla sicurezza e revisione medica. La maggior parte dei dati raccolti durante la Studio sono salvati nel database clinico gestito dai soggettiche lavorano per conto dello sponsor, il Titolare del trattamento dei dati. Questi soggettidispongono di misure di sicurezza proprie. Al termine dello studio, i dati personali raccolti n e l database clinico vengono archiviati. Significa che il database è bloccato ed è impossibile qualsiasi modifica dei dati	Limitato	Trascurabile

Scomparsa dei dati	Errore umano (dipendente interno) Fallimento in Sistema IT Disastro: distruzione dei server	Cancellazione accidentale / Scomparsa dei dati	E' già in atto un controllo per limitare le minacce. Alcune di queste misure sono migliorabili per aumentare il livello di protezione dei dati per quanto riguarda la scomparsa dei dati. e. Tutti i dati personali raccolti durante lo studio clinico e inseriti nel database clinico sono inseriti dal personale dello studio utilizzando i documenti di partenza disponibili in loco. In caso di scomparsa dei dati, il rischio per le persone interessate è trascurabile in quanto il database potrebbe essere ricostruito sulla base dei documenti di origine	Sicurezza informatica e salvaguardia in atto. Procedure organizzative (autorizzazione del personale, rapporto con terzi) Tracciabilità (registro degli accessi) Procedure generali di sicurezza del sistema (sicurezza delle operazioni e gestione delle postazioni di lavoro) Protezione contro fonti di rischio non umane in atto Incidente /gestione delle violazioni dei dati con l'implementazione di una procedura di allerta. A seconda della decisione relativa all' incidente/alla violazione dei dati, i soggetti interessati o il loro rappresentante legale devono essere informato	Limitato	Trascurabile

Mappatura dei rischi legati alla sicurezza dei dati

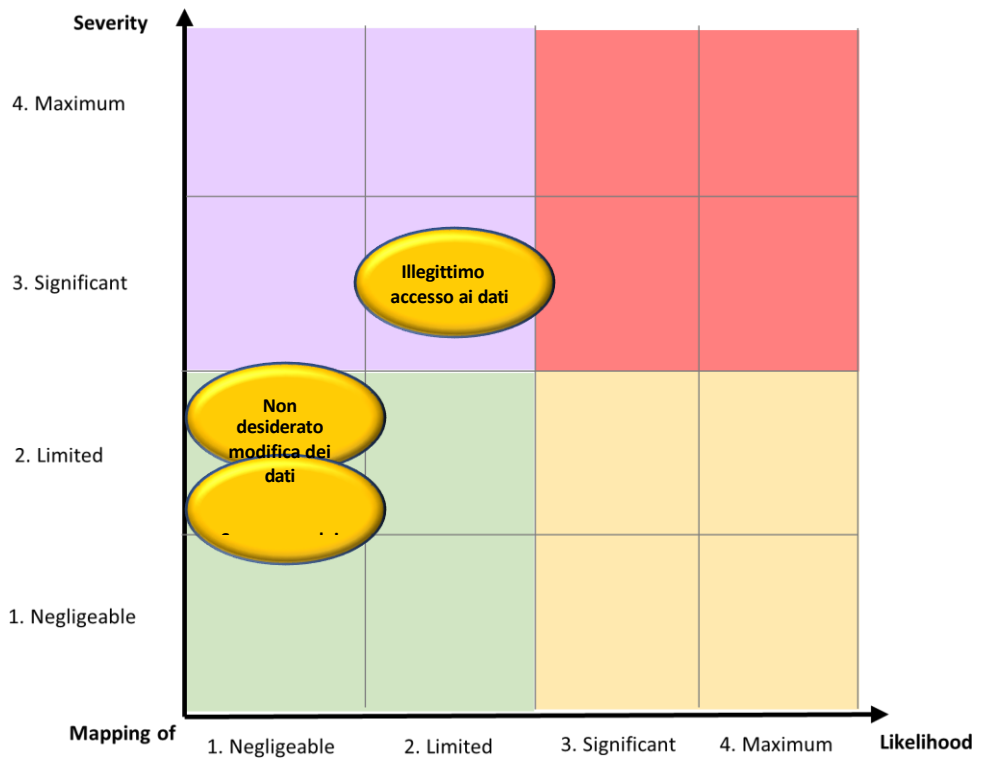


Grafico del flusso di lavoro dei dati

Il diagramma del flusso di lavoro dei dati dello studio Ebvolve è descritto nell'**Appendice 3.**

VALIDAZIONE FORMALE DELLA DPIA

Alla luce delle informazioni fornite nel presente documento e in considerazione delle modalità di trattamento dei dati sopra descritte, il Responsabile della Protezione dei Dati concorda con la valutazione dello Sponsor.

La finalità del trattamento è la ricerca scientifica e il pubblico interesse per descrivere e caratterizzare il profilo di sicurezza ed efficacia di tabelecleucel in soggetti con PTLD da EBV+.
dopo un trapianto di cellule ematopoietiche (HCT) o un trapianto di organi solidi (SOT), in un contesto reale in Europa.

Le misure previste per rispettare i principi fondamentali della privacy e per affrontare i rischi per la privacy dei soggetti sono considerate accettabili alla luce di questo problema. Tuttavia, ~~il~~
dovrà essere dimostrata l'implementazione di misure aggiuntive, nonché il continuo miglioramento della DPIA.

Più specificamente, per quanto riguarda l'Italia:
come già precisato nel presente documento, con la recente modifica dell'Art.110 Codice Privacy, per i trattamenti di dati personali concernenti la ricerca medica, biomedica ed epidemiologica, nei casi in cui sia impossibile ottenere il consenso dell'interessato, l'obbligo di consultazione preventiva al Garante è stato sostituito con l'l'osservanza delle garanzie individuate dallo stesso Garante, ai sensi dell'art. 106 comma 2, lettera d) Codice privacy., e previste anche dalle regole deontologiche definite dal Garante per i soggetti pubblici e privati, inerenti al trattamento dei dati per fini statistici o di ricerca scientifica, volte ad individuare garanzie adeguate per i diritti e le libertà dell'interessato, in conformità dell'Art.89 GDPR.
Alla luce di ciò, il DPO raccomanda di monitorare le attività del Garante volte all'adozione di regole deontologiche applicabili allo studio oggetto della presente DPIA; qualora future regole deontologiche comportassero la necessità di modificare alcuni aspetti del trattamento posto in essere, il Titolare dovrà immediatamente adeguarsi a tali previsioni e aggiornare la presente DPIA

Pierre-André POIRIER, Responsabile della protezione dei dati personali

08-giugno.-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

APPENDICI

Appendice 1: Pratiche di sicurezza aziendale Oracle settembre 2023 v3.2

Appendice 2: Documentazione di Oracle® Life Sciences Clinical One Cloud Service (Clinical One)

- **Appendice 2a**: OLS C1_Regolamentazione_Conformità_Addendum_V6_FINALE
- **Appendice 2b**: Controlli tecnici, organizzativi e procedurali
  (Guida alle caratteristiche del prodotto Oracle_Life_Sciences_Clinical_One_Cloud_Service) Luglio_2023)

Appendice 3: Tabella del flusso di lavoro EBVOLVE_Data_20240320

Appendice 4: DPIA Go Cell Terapy