

# VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

## Contesto

### Panoramica

#### Qual è il trattamento in esame?

La raccolta di dati personali relativi a pazienti e operatori sanitari nell'ambito dello studio VINOREAL (di seguito lo "Studio").

VINOREAL è uno studio multicentrico, multinazionale, retrospettivo e prospettico, osservazionale, volto a descrivere gli attuali dati di efficacia e sicurezza nel mondo reale dei trattamenti a base di OV, nonché il percorso sanitario e la qualità di vita (QoL) del paziente associati a questo trattamento di pazienti con cancro al seno avanzato (ABC) utilizzando i questionari FACT-B, PPQ e WPAI.

Lo studio sarà condotto in 3 Paesi : Italia, Algeria e Cina.

La popolazione dello studio sarà composta da:

- Pazienti arruolati retrospettivamente, ovvero pazienti di età  $\geq 18$  anni ( $\geq 19$  anni per l'Algeria, come da normativa locale) al momento dell'inizio del trattamento a base di OV che hanno iniziato il trattamento con OV per l'ABC tra il 2011 e il 2020.
- Pazienti arruolati prospetticamente, ovvero pazienti di età  $\geq 18$  anni ( $\geq 19$  anni per l'Algeria, come da normativa locale) all'inizio del trattamento a base di OV, che iniziano il trattamento con OV al momento dell'inclusione nello studio o successivamente, ed eleggibili per la raccolta prospettica dei dati sulla QoL e dei questionari PPQ e WPAI.

In considerazione di quanto sopra, Pierre Fabre Medicament tratterà i dati personali relativi a:

- Pazienti viventi che hanno dato il loro consenso firmando il modulo di consenso informato e che non si sono opposti al trattamento dei dati personali, avendo letto l'Informativa sul trattamento dei dati personali effettuato da Pierre Fabre nel contesto dello studio, e,
- Pazienti deceduti per i quali l'Informativa sulla Privacy può essere resa disponibile, e il relativo Modulo di Consenso Informato può essere firmato da un rappresentante legale e per l'Italia, in base all'art. 110 del D.Lgs. 196/2003 (di seguito, il "Codice Privacy"), come ulteriormente modificato dall'art. 44 co 1 bis l. 29/04/2024 n. 56 come meglio precisato nel presente documento.

## **Quali sono le responsabilità legate al trattamento?**

- Pierre Fabre Medicament S.A.(Pierre Fabre), società con sede legale a Les Cauquillous - 81500 Lavaur (Francia), agisce in qualità di sponsor dello Studio e, titolare del trattamento dei dati personali degli Interessati nell'ambito dello StudioFortrea France S.a.r.l., con sede legale in 2 rue Jacque Daguerre, 92500 Rueil-Malmaison (Francia), agisce in qualità di Responsabile del trattamento dei dati debitamente designato da Pierre Fabre attraverso un Accordo di trattamento dei dati ai sensi dell'articolo 28 del GDPR, che in qualità di CRO assiste Pierre Fabre Medicament nella gestione delle attività relative allo Studio (tra cui, i rapporti con i comitati etici e le istituzioni dei Siti, la raccolta e la trasmissione dei dati personali pseudonimizzati dei Pazienti, la raccolta e la gestione dei dati e la comunicazione finale dei risultati pseudonimizzati, ecc.), agendo come responsabile del trattamento dei dati.
- I Siti, compresi gli ospedali e i centri medici che partecipano allo Studio, nonché i medici curanti (sperimentatori) esperti nella somministrazione di farmaci antitumorali e nella prescrizione di trattamenti ai Pazienti, agiscono in qualità di Titolare del trattamento dei file medici relativi ai partecipanti allo studio.
- Eventuali fornitori terzi dell'infrastruttura tecnologica utilizzata dallo Sponsor per l'esecuzione dello Studio che, in ogni caso, non hanno accesso ai dati trattati.
- 

## **Esistono norme applicabili al trattamento?**

A questo trattamento si applicano le norme europee e nazionali relative alle buone pratiche cliniche (GCP europee) e le norme sulla privacy dei dati (GDPR e norme nazionali sulla protezione dei dati).

## **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, PF 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 PF (<https://clinicaltrials.pierre-fabre.com>) 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 deceduti i centri compiono sforzi ragionevoli per ottenere il consenso da parte dei loro legali rappresentanti contattandoli all'ultimo indirizzo conosciuto. Il centro riporta nelle cartelle cliniche dei pazienti.
- Per i pazienti deceduti e 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 PF e sul sito web del Centro, nonché affissa nella sala d'attesa del Centro, quando possibile, consentendo agli interessati di avere accesso all'Informativa sulla privacy ed esercitare i propri diritti.

## Contesto

### Dati, processi e asset di supporto

#### Quali sono i dati trattati?

Se disponibili, verranno raccolti i seguenti dati chiave:

- Caratteristiche demografiche e cliniche dei pazienti alla diagnosi iniziale di ABC o all'inizio del trattamento con OV (entrambe le coorti).
- Anamnesi di trattamento per cancro al seno e ABC dalla diagnosi e prima dell'inizio del trattamento OV (entrambe le coorti).
- Trattamento OV per il cancro al seno avanzato (entrambe le coorti) dall'inizio del trattamento all'interruzione definitiva.
- Trattamenti antitumorali concomitanti: data di inizio, data di fine, dose, motivo della modifica/interruzione/interruzione della dose per ogni dose di trattamento somministrata e per ogni interruzione del trattamento.
- Esito clinico dopo l'interruzione permanente di OV (entrambe le coorti).
- Eventi avversi (entrambe le coorti).
- Linea/e di trattamento successiva/e per il tumore al seno dopo l'interruzione del trattamento con vinorelbina orale (entrambe le coorti).
- Accesso e percorso sanitario (entrambe le coorti).
- Dati sulla QoL solo per i pazienti inclusi prospetticamente.
- Preferenza dei pazienti per la via di somministrazione del trattamento solo per i pazienti inclusi prospetticamente.
- Produttività lavorativa solo per i pazienti inclusi prospetticamente.

#### Chi sono i soggetti interessati dal Processo e qual è il numero di soggetti che si prevede saranno impattati da questo Processo?

Il processo prevede il trattamento di circa 368 pazienti partecipanti allo studio:

- 130 pazienti retrospettivi (di cui 40 per l'Italia)
- 238 pazienti prospettici (di cui 30 per l'Italia)

I siti italiani che partecipano allo Studio sono i seguenti:

- Sito n. 38001 - IRCCS San Gerardo dei Tintori, centro di ricerca di fase 1 - Data di approvazione 29 febbraio 2024
- Sito n. 38003 - Ospedale San Martino di Belluno, UOC Oncologia - Data di approvazione 29 febbraio 2024
- Sito n. 38004 - IRCCS Ospedale Policlinico San Martino - Data di approvazione 29 febbraio 2024

In particolare, la popolazione dello studio sarà composta da:

- I pazienti arruolati retrospettivamente, ovvero i pazienti che hanno iniziato il trattamento OV per ABC tra il 2011 e il 2020, saranno arruolati nello studio di coorte retrospettivo. Il periodo di osservazione per i pazienti inclusi retrospettivamente si estenderà dall'inizio del trattamento OV alla data di morte, alla data dell'ultimo contatto o alla data di fine del periodo di osservazione retrospettiva, a seconda di quale si verifichi per prima. La data di fine del periodo di osservazione retrospettiva sarà fissata come data di inclusione del primo paziente nello studio (First Patient In= FPI).
- I pazienti arruolati in modo prospettico, ovvero i pazienti che iniziano il trattamento con OV e sono idonei alla raccolta prospettica dei dati sulla QoL e dei questionari PPQ e WPAI, saranno arruolati nello studio di coorte prospettico. Il periodo di arruolamento dovrebbe estendersi fino a 17 mesi dall'inizio dello studio. Il periodo di osservazione dello studio si estenderà fino a 2 anni dopo l'ultima visita del paziente (circa 24 mesi dopo l'inizio del trattamento).

In considerazione di quanto sopra, Pierre Fabre tratterà i dati personali relativi a:

- Pazienti viventi che hanno dato il loro consenso al trattamento dei dati personali firmando il modulo di consenso informato, avendo preso visione dell'Informativa sulla privacy relativa al trattamento dei dati personali effettuato da Pierre Fabre nell'ambito dello Studio per l'Italia come per l'Algeria e la Cina, alcuni siti possono beneficiare di deroghe; e

- Pazienti deceduti per i quali l'Informativa sulla Privacy può essere resa disponibile e il relativo Modulo di Consenso Informato può essere ottenuto da un avente causa, dal legale rappresentante o da chiunque agisca per conto del defunto in qualità di suo rappresentante o, per l'Italia, in base all'art. 110 del D.Lgs. n. 196/2003, come ulteriormente modificato dall'art. 44 co 1 bis l. 29/04/2024 n. 56 (di seguito, il "Codice della Privacy") come meglio precisato nel presente documento.

In ogni caso, per essere eleggibili allo studio, i pazienti devono avere un'età inferiore ai 18 anni ( $\geq 19$  anni per l'Algeria, come previsto dalla normativa locale) al momento dell'inizio del trattamento a base di OV.

Quando i pazienti accettano di partecipare allo studio, vengono eseguite le seguenti fasi:

1) Raccolta e inserimento dei dati da parte degli investigatori dei siti - A questo scopo, i dati raccolti

dalle cartelle cliniche dei pazienti saranno inseriti dai siti in un case report elettronico separato per ogni paziente, il modulo "electronic Case Report Form" ("eCRF"). Ai pazienti arruolati in modo prospettico verrà consegnato un diario cartaceo al momento dell'inclusione, contenente le istruzioni e il calendario per la compilazione dei questionari, nonché il lotto di questionari in bianco da compilare secondo il calendario specifico. Lo sperimentatore del sito o un suo incaricato qualificato registrerà le risposte nell'eCRF.

2) Pseudonimizzazione dei dati - I siti caricheranno i dati nell'Electronic Data Capture ("EDC"), sistema che lo Sponsor, per mezzo della CRO, utilizzerà per archiviare e analizzare i dati raccolti.

Il CDE conserverà i dati personali pseudonimizzati (codificati con chiavi) solo per non permettere che la

Sponsor (e quindi la CRO) di identificare direttamente i pazienti. Infatti, solo il sito pertinente hanno accesso sia all'ID del paziente che alle informazioni direttamente identificabili di ciascun paziente.

Lo Sponsor (e la CRO), invece, non avrà accesso ai dati identificativi di ciascun paziente, compresi nome e cognome, e non sarà in grado di collegare l'ID di ciascun paziente con il relativo

paziente, poiché i dati inseriti nell'EDC dai siti saranno già codificati con codici chiave e quindi pseudonimizzati.

3) Processo di analisi dei dati - I dati inseriti nell'eCRF saranno esaminati per verificarne la coerenza da parte della

competente che utilizza sia controlli logici automatizzati (cioè l'emissione di interrogazioni automatiche), sia controlli di sicurezza.

generati dal sistema) e la revisione manuale (cioè l'emissione di controlli manuali impostati dal sistema).

manager o il monitor nell'eCRF). Tutti i dati raccolti nell'eCRF saranno approvati e firmati elettronicamente e datati dallo sperimentatore o da un suo incaricato. Questa approvazione attesta la revisione e l'accettazione da parte dello sperimentatore della completezza e dell'accuratezza dei dati. Al termine dello studio e prima dell'analisi statistica finale, l'e-CRF e gli altri dati dello studio saranno bloccati per evitare ulteriori aggiunte o correzioni. Il blocco dei dati dello studio rappresenta la conferma che tutti i dati sono stati acquisiti e confermati come accurati.

4) Redazione della relazione di studio - I dati analizzati saranno documentati in una relazione di studio e

comunicati, in modo aggregato, da Fortrea a Pierre Fabre Medicament. Questa fase sarà svolta da Fortrea, per conto di Pierre Fabre Medicament. I rappresentanti della garanzia di qualità di Fortrea o di Pierre Fabre Medicament possono visitare un Sito per condurre una verifica di garanzia di qualità e garantire che lo Studio sia condotto in conformità con il Protocollo, le Procedure Operative Standard (SOP) e tutti i requisiti di legge applicabili.

5) Conservazione dei dati - Pierre Fabre Medicament conserva il rapporto di studio per 25 anni dal termine dello studio per i motivi meglio indicati di seguito. In ogni caso, al termine di questo periodo di conservazione, i dati saranno cancellati o resi irreversibilmente anonimi o aggregati.

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

1. La raccolta e l'inserimento dei dati sono eseguiti dagli sperimentatori.
2. Il CED esegue la pseudonimizzazione fornendo un numero di paziente univoco per ogni paziente inserito nel CED.
3. Pulizia dei dati da parte degli investigatori e di Fortrea
4. Analisi dei dati da parte di Fortrea
5. Redazione del rapporto di studio da parte di Fortrea
6. Rapporto sullo studio dei dati aggregati inviato a Pierre Fabre Medicament
7. Pierre Fabre Medicament archiviazione per 25 anni a partire dalla fine dello studio.

## **Quali sono i dati a supporto degli asset?**

I dati personali saranno trattati attraverso i seguenti sistemi:

- eCRF (electronic Clinical Report File) archiviato sui server Medidata come EDC
- Gli estratti del CDE sono condivisi su Share Drive di Fortrea e, se necessario, condivisi con Pierre Fabre Medicament sull'MFT in base al DTA statistico.
- Le analisi vengono eseguite e i dati per le analisi sono ospitati dal SAS Hosted Environment con analisi condotte su SAS Enterprise Guide (cioè, SAS v9.4 o successivo).
- La scrittura della RSI avverrà su server Fortrea.
- Studio VINOREAL di Pierre Fabre Medicament in SharePoint, che contiene i documenti dello studio utilizzati solo con gli stakeholder interni di Pierre Fabre Medicament su base strettamente necessaria.
- Sharedoc di Pierre Fabre Medicament, utilizzato da Fortrea per condividere l'analisi statistica (ad esempio, tabelle, figure ed elenchi) con Pierre Fabre Medicament. L'accesso a tale sistema è concesso da Pierre Fabre Medicament a Fortrea che carica esclusivamente l'analisi.
- ZEC Pierre Fabre Biometrie, utilizzato da Pierre Fabre Medicament solo per l'archiviazione dei documenti dello studio.

La CRO garantirà che le CRF siano conservate in modo sicuro presso la sede di ricerca della CRO in forma elettronica criptata e saranno protette da password o messe al sicuro in una stanza chiusa a chiave per impedire l'accesso a terzi non autorizzati.

# **Principi fondamentali**

## **Proporzionalità e necessità**

### **Le finalità del trattamento sono specificate, esplicite e legittime?**

L'obiettivo dell'elaborazione dei dati è principalmente quello di descrivere gli attuali dati di efficacia e sicurezza nel mondo reale dei trattamenti a base di OV, nonché il percorso sanitario del paziente e la qualità di vita (QoL) associata a questo trattamento dei pazienti con ABC utilizzando i questionari FACT-B, PPQ e WPAI.

## Quali sono le basi giuridiche che rendono lecito il trattamento?

- Con specifico riferimento all'Italia, Pierre Fabre tratta i dati personali dei Pazienti sulla base di:
  - il previo consenso del Paziente ai sensi dell'articolo 9, paragrafo 2, lettera a), del GDPR per categorie particolari di dati personali (ad esempio, dati sanitari ed eventi avversi del trattamento). Questo consenso viene fornito in aggiunta al Modulo di Consenso Informato ("ICF") che lo Sponsor richiede ai Pazienti per accettare di partecipare allo Studio. In particolare, il sito fornirà ai pazienti un'informativa scritta sul trattamento dei dati personali nell'ambito dello studio prima dell'estrazione dei dati dalle cartelle cliniche dei pazienti. Se i pazienti accettano di partecipare allo studio, verrà chiesto loro di fornire anche il consenso scritto ai fini di privacy per i pazienti deceduti,

(i) sul consenso espresso dai loro aventi causa ai quali l'Informativa sulla privacy può essere resa disponibile e il relativo modulo di consenso informato può essere firmato da un avente causa, dal rappresentante legale o da chiunque agisca per conto della persona deceduta in qualità di suo rappresentante; oppure

(ii) solo nel caso in cui non sia stato possibile ottenere il consenso al trattamento dei dati da parte dei loro aventi causa, sulla base dell'art. 110 del Codice Privacy che prevede che, qualora non sia possibile contattare gli interessati per ottenere il consenso o ciò comporti uno sforzo sproporzionato o il rischio di compromettere le finalità dello Studio, il titolare del trattamento deve ottenere il parere favorevole motivato del comitato etico competente, rendere pubblica una valutazione d'impatto sulla protezione dei dati e comunicarla al Garante per la protezione dei dati personali, in conformità al provvedimento del Garantedel 9 maggio2024.

Pertanto, con riferimento ai pazienti deceduti, la base giuridica del trattamento è il consenso se gli aventi causa sono contattabili, e l'articolo 110 del Codice della privacy in caso contrario. Per contattare gli aventi causa dei pazienti deceduti, Pierre Fabre compie sforzi ragionevoli verificando se il Sito è in grado di mettersi in contatto con questi ultimi. Solo nel caso in cui tali tentativi di contatto non vadano a buon fine, Pierre Fabre , in applicazione dell 'articolo 110 del Codice della privacy pubblicherà un'informativa sul proprio sito web e sul sito web del Centro, chiedendo altresì affissa nella sala d'attesa del Centro ove possibile.

- Legittimo interesse del titolare del trattamento (per i siti algerino e cinese) derivante dalla conoscenza delle condizioni di vita delle persone in trattamento per il trattamento dei dati relativi allo Studio,
- Esecuzione del contratto con i siti di studio (sperimentatori),
- Obbligo legale di attività di vigilanza

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

Tutti i dati raccolti sono adeguati, pertinenti e limitati agli obiettivi dello studio, che sono i seguenti:

L'obiettivo dello studio è quello di descrivere gli attuali dati di efficacia e sicurezza nel mondo reale dei trattamenti a base di OV, nonché il percorso sanitario e la qualità di vita (QoL) dei pazienti associati a questo trattamento di pazienti con carcinoma mammario avanzato.

- Obiettivo primario:
  - Descrivere l'efficacia in termini di sopravvivenza libera da progressione (PFS) a 2 anni di follow-up del trattamento a base di OV in pazienti con ABC, in coorti retrospettive e prospettiche.
- Obiettivi secondari:
  - Descrivere l'efficacia in termini di sopravvivenza globale (OS) a 2 anni di follow-up del trattamento a base di OV in pazienti con ABC in coorti retrospettive e prospettiche.
  - Descrivere l'efficacia in termini di PFS e OS di OV nei pazienti con ABC nella coorte retrospettiva.
  - Descrivere le caratteristiche cliniche e demografiche e le comorbidità dei pazienti con ABC trattati con terapia a base di OV in qualsiasi linea di trattamento in un contesto reale e in base ai marcatori molecolari (stato HR, stato HER2) in coorti retrospettive e prospettiche.
  - Descrivere il profilo di sicurezza osservato e la frequenza degli eventi avversi (AE) rilevanti nei pazienti con ABC trattati con un trattamento a base di OV in qualsiasi linea di trattamento in coorti retrospettive e prospettiche.
  - Descrivere i modelli di trattamento nel mondo reale (compresi i precedenti trattamenti antitumorali per il cancro al seno) dei pazienti con ABC trattati con un trattamento a base di OV in qualsiasi linea di trattamento, compresi la dose di trattamento, la durata del trattamento, le interruzioni permanenti e temporanee, i motivi delle interruzioni e i trattamenti concomitanti in coorti sia retrospettive che prospettiche.
  - Descrivere l'accesso all'assistenza sanitaria e il percorso dei pazienti con ABC trattati con un trattamento a base di OV in qualsiasi linea di trattamento, valutato attraverso ospedalizzazioni, radioterapie e interventi chirurgici in coorti retrospettive e prospettiche.
  - Valutare l'evoluzione della QoL di pazienti prospettiche con ABC trattate con un trattamento a base di OV in un contesto reale utilizzando il Functional Assessment of Cancer Therapy - Breast (FACT-B), uno strumento che misura lo stato di salute delle pazienti affette da cancro al seno.
  - Valutare la preferenza dei pazienti prospettici con ABC per la via di somministrazione di OV, utilizzando un questionario sulle preferenze dei pazienti (PPQ).
  - Valutare l'impatto del cancro sulla produttività lavorativa e sulle attività quotidiane di pazienti prospettici con ABC trattati con OV per qualsiasi linea di trattamento in un contesto reale, utilizzando il questionario Work Productivity and Activity Impairment (WPAI).

## **I dati sono accurati e aggiornati?**

La fonte dei dati da esaminare durante lo studio comprende le cartelle cliniche dei pazienti, i questionari (se applicabili), gli esami di laboratorio originali, i referti istologici e patologici.

La CRO ha la responsabilità ultima, per conto di Pierre Fabre Medicament che agisce in qualità di Sponsor, di raccogliere e riportare tutti i dati clinici, di sicurezza e di laboratorio inseriti nelle eCRF e in qualsiasi altro modulo di raccolta dati (documenti di partenza) e di garantire che siano accurati, autentici/originali, attribuibili, completi, coerenti, leggibili, tempestivi (contemporanei), duraturi e disponibili quando richiesto.

In particolare, le eCRF sono approvate con una firma elettronica (le modifiche ai dati precedentemente inviati richiedono una nuova firma elettronica per confermare/approvare le modifiche). I dati inseriti nell'eCRF saranno esaminati per verificarne la coerenza dal responsabile dei dati, utilizzando sia controlli logici automatizzati (cioè emettendo query automatiche generate dal sistema) sia revisioni manuali (cioè emettendo controlli manuali impostati dal responsabile dei dati o dal monitor nell'eCRF). Per ogni incongruenza rilevata, verrà generata un'interrogazione specifica dell'eCRF (automatica o manuale) e lo sperimentatore o lo specialista dell'inserimento dei dati sarà responsabile della correzione o dell'aggiornamento delle informazioni non corrette o incomplete. Per ridurre al minimo il numero di dati mancanti, verrà generata un'interrogazione specifica (automatica o manuale) per confermare che i dati sono veramente mancanti piuttosto che essere una voce trascurata nella eCRF. Un audit trail all'interno del sistema terrà traccia di tutte le modifiche apportate ai dati.

La CRO o i siti sono responsabili della verifica delle eCRF a intervalli regolari nel corso dello Studio per verificare l'aderenza al protocollo e alle SOP applicabili dello Sponsor, la completezza, l'accuratezza e la coerenza dei dati e l'aderenza alle normative locali sulla conduzione della ricerca clinica.

Durante e/o dopo il completamento dello Studio, i revisori della qualità nominati dallo Sponsor o dalle autorità regolatorie possono eseguire verifiche in loco, ispezionando anche le varie registrazioni dello Studio (ad esempio, gli e-CRF e altri dati pertinenti), a condizione che venga rispettata la riservatezza del paziente.

## **Qual è la durata di conservazione dei dati?**

La durata di conservazione del Titolare del trattamento è di 25 anni a partire dalla data di conclusione dello studio.

L'archiviazione locale per ogni centro di studio è di 15 anni (soggetta a variazioni locali per rispettare la normativa locale) dalla data di fine dello studio.

# Principi fondamentali

## Controlli per la tutela dei diritti personali degli interessati

### Come vengono informati gli interessati del trattamento?

Pierre Fabre fornisce un'informativa sulla privacy ai sensi dell'art. 13 del GDPR ai pazienti che partecipano allo Studio e che forniscono il loro consenso secondo le modalità e le procedure previste dalle Linee guida per il trattamento dei dati nell'ambito delle sperimentazioni cliniche di farmaci - 24 luglio 2008 [doc. web. n. 1671330].

In alcuni casi (ad esempio, pazienti deceduti), tuttavia, Pierre Fabre è esonerato dall'obbligo di fornire direttamente agli interessati un'informativa sulla privacy, poiché ciò rappresenterebbe uno sforzo sproporzionato ai sensi dell'articolo 14, paragrafo 5, e del considerando 62 del GDPR. Questa disposizione ha chiarito che: *"Tuttavia, non è necessario imporre l'obbligo di fornire informazioni quando l'interessato è già in possesso delle informazioni, quando la registrazione o la divulgazione dei dati personali è espressamente prevista dalla legge o quando la fornitura di informazioni all'interessato si rivela impossibile o comporterebbe uno sforzo sproporzionato. Quest'ultimo caso potrebbe verificarsi in particolare quando il trattamento viene effettuato per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. A questo proposito, occorre prendere in considerazione il numero degli interessati, l'età dei dati e le garanzie adeguate adottate."*

In effetti, va notato che contattare gli interessati ai fini dello studio comporterebbe uno sforzo sproporzionato per Pierre Fabre per i seguenti motivi:

- a) lo studio deve essere condotto retrospettivamente su pazienti che hanno iniziato un trattamento con OV per un tumore al seno avanzato, tra il 2011 e il 2020; e
- b) il numero massimo stimato di soggetti interessati è fino a 130 pazienti retrospettivi che nella maggior parte dei casi potrebbero essere deceduti durante i trattamenti clinici.

Per quanto riguarda le garanzie poste in essere da Pierre Fabre ai sensi dell'art. 44 co 1° della Legge 29/04/2024 n. 56, i motivi di cui sopra devono essere considerati come ragioni di impossibilità organizzativa di informare i pazienti interessati, come previsto dall'Autorità Garante della Privacy nel suo Provvedimento del 9 maggio 2024, : i) la mancata raccolta dei dati relativi ai pazienti interessati che non possono essere contattati, rispetto al numero totale di soggetti da arruolare nello studio, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della ricerca; ii) in via residuale, contattare tutti i pazienti interessati comporterebbe uno sforzo sproporzionato dato il numero particolarmente elevato di soggetti interessati.

In ogni caso, l'Informativa sulla Privacy di cui agli artt. 13 e 14 del GDPR e relativa al trattamento dei dati personali effettuato nell'ambito dello Studio sarà disponibile anche agli aventi diritto dei pazienti deceduti sul sito web di Pierre Fabre all'indirizzo: <https://clinicaltrials.pierre-fabre.com/en/vinoreal/> unitamente alla presente DPIA.

## **Se applicabile, come viene ottenuto il consenso degli interessati?**

Lo sperimentatore informerà i pazienti vivi (o i parenti stretti/rappresentanti legali nel caso in cui il paziente sia deceduto, se applicabile) sulla natura, lo scopo e le conseguenze della loro partecipazione. Ai pazienti (o ai parenti stretti/rappresentanti legali, se del caso) verrà consegnato il modulo di informazione per il paziente attualmente approvato, che dovrà essere letto, e verranno affrontate tutte le domande che potrebbero sorgere.

I pazienti (o i loro parenti stretti/rappresentanti legali, se del caso) saranno debitamente informati degli obiettivi dello studio e della possibilità di rifiutare o interrompere la loro partecipazione allo studio senza alcun pregiudizio per il loro rapporto con lo sperimentatore e la loro gestione medica. I pazienti (o i parenti prossimi/rappresentanti legali, se del caso) saranno inoltre informati dei loro diritti in merito al trattamento dei dati personali. Saranno applicate rigorosamente tutte le leggi, i regolamenti e i requisiti CE applicabili.

Dopo aver ottenuto il consenso alla partecipazione da parte del paziente (o del parente più prossimo/rappresentante legale, se applicabile), lo sperimentatore potrà raccogliere i dati di base richiesti nell'eCRF.

Lo sperimentatore documenterà, nella cartella clinica del paziente, il consenso informato, il rifiuto, la non opposizione o l'opposizione alla partecipazione allo studio del paziente (o del rappresentante legale del parente più prossimo), prima di procedere alla raccolta dei dati (se applicabile).

Lo sperimentatore compilerà un registro di screening delle pazienti per registrare tutte le pazienti invitate a partecipare e i motivi della mancata inclusione. Il registro di screening delle pazienti sarà utilizzato per valutare la rappresentatività del campione dello studio e i dati da raccogliere in tale registro possono includere l'età della paziente, lo stadio del tumore al seno e il motivo della mancata inclusione, se applicabile. Per coloro che si sono rifiutati di partecipare allo studio, verranno registrati i motivi del rifiuto.

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

I pazienti possono esercitare in qualsiasi momento i loro diritti alla privacy e, in particolare:

- Diritto di accesso in base al quale i pazienti hanno il diritto di richiedere l'accesso ai propri dati personali (articolo 15 del GDPR) tramite l'indirizzo generico del Responsabile della protezione dei dati (DPO) dello Sponsor: [dpofr@pierre-fabre.com](mailto:dpofr@pierre-fabre.com).

I pazienti italiani possono esercitare il diritto alla portabilità dei dati (articolo 20 del GDPR) utilizzando lo stesso indirizzo e-mail sopra indicato.

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

I pazienti possono esercitare in qualsiasi momento i loro diritti alla privacy e, in particolare:

- Diritto di rettifica, in base al quale i pazienti hanno il diritto di richiedere la rettifica di eventuali dati personali incompleti o inesatti in possesso di Pierre Fabre Medicament (articolo 16 del GDPR);

- Diritto alla cancellazione, in base al quale i pazienti hanno il diritto di richiedere la cancellazione dei dati raccolti dallo Sponsor, a meno che la cancellazione non renda impossibile o metta seriamente a rischio il raggiungimento degli obiettivi della ricerca (articolo 17 del GDPR); e

Per esercitare tali diritti alla privacy, i pazienti possono:

- 1) mettersi in contatto con il sito, il medico dello studio o l'équipe di ricerca, che provvederà a indirizzare il problema al responsabile della protezione dei dati dello Sponsor, oppure
- 2) Contattare direttamente il Responsabile della Protezione dei Dati (DPO) dello Sponsor inviando una e-mail al seguente indirizzo: [dpofr@pierre-fabre.com](mailto:dpofr@pierre-fabre.com)

Per l'Italia e ai sensi dell'art. 2-terdecies del Codice Privacy, in caso di decesso del Paziente, i suddetti diritti potranno essere esercitati da soggetti portatori di un interesse proprio, o che agiscono in qualità di rappresentanti del paziente, o per ragioni familiari meritevoli di tutela. Prima della sua morte, il Paziente può vietare espressamente l'esercizio di alcuni dei diritti sopra elencati da parte dei suoi aventi diritto, inviando una dichiarazione scritta allo Sponsor o al Sito secondo le modalità sopra indicate. Tale dichiarazione potrà essere revocata o modificata successivamente con le stesse modalità.

In ogni caso, ai fini dello studio saranno trattati solo dati personali pseudonimizzati. Pertanto, Pierre Fabre Medicament potrebbe non essere in grado di rispondere alle richieste degli Interessati qualora la risposta a tali richieste richieda dati identificabili.

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

In conformità alle disposizioni del GDPR, gli interessati possono esercitare in qualsiasi momento i seguenti diritti:

- Diritto alla limitazione in base al quale i pazienti hanno il diritto di chiedere allo Sponsor di sospendere il trattamento di alcuni dati personali, qualora (i) l'accuratezza dei dati personali sia contestata dai pazienti, per un periodo che consenta allo Sponsor di verificare l'accuratezza dei dati personali, (ii) il trattamento sia illegale, e l'interessato si oppone alla cancellazione dei dati personali e chiede invece la limitazione del loro utilizzo, e (iii) lo Sponsor non ha più bisogno dei dati personali per le finalità del trattamento, ma sono richiesti dall'interessato per l'istituzione, l'esercizio o la difesa di rivendicazioni legali (articolo 18 del GDPR).
- Diritto di opposizione, in base al quale i pazienti possono opporsi in qualsiasi momento al trattamento dei loro dati personali. In questo caso non verranno raccolti nuovi dati. ( Nota per l'Italia : poiché la base giuridica è il consenso dei Pazienti, qualora questi ultimi decidano di partecipare allo Studio, avranno la possibilità di ritirare il proprio consenso in qualsiasi momento, senza pregiudicare il trattamento dei dati personali effettuato prima del ritiro del consenso. In questo caso, non verranno più raccolti dati.

**Gli obblighi degli incaricati del trattamento sono chiaramente identificati e regolati da un contratto?**

Un contratto quadro è stato firmato da e tra Pierre Fabre Medicament (in qualità di Titolare del trattamento dei dati) e Fortrea (in qualità di Responsabile del trattamento dei dati) il 20 aprile 2023 (riferimento documento: CRO 2023-00329\_NIS Navelbine\_728094\_Services Agreement\_Final).

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

In caso di trasferimento di dati al di fuori dell'Unione Europea, tutti i dati raccolti sono debitamente protetti (i) dalla stipula di Clausole Contrattuali Standard (SCC) come emanate dalla Commissione Europea (edizione giugno 2021) in caso di trasferimento di dati al di fuori dello Spazio Economico Europeo ("SEE") e verso un paese non approvato dalla Commissione Europea come fornitore di protezione adeguata ai sensi dell'articolo 45 del GDPR o (ii) attraverso una delle deroghe per situazioni specifiche elencate nell'articolo 49 del GDPR.

# I rischi

**A) Valutazione dei rischi per i diritti e le libertà degli interessati (art. 37, comma 7, lett. c) del GDPR)** I principali e maggiori rischi individuati sono i seguenti:

- Accesso illegittimo ai dati
- Modifica indesiderata dei dati
- Scomparsa dei dati

**La partecipazione allo studio non comporta rischi per la salute. In particolare, lo studio non comporterà alcuna modifica degli standard di assistenza locale dei soggetti dello studio, non comprometterà la loro integrità fisica o psicologica e non richiederà visite di follow-up speciali per questi soggetti dello studio.**

Tuttavia, il trattamento dei dati derivante dal processo sopra descritto può comportare i seguenti rischi per i diritti e le libertà degli Interessati:

- a) l'accesso ai dati personali dei soggetti dello studio senza che questi ne siano consapevoli, compresi i dati relativi alla salute, e la relativa perdita di riservatezza; e
- b) l'utilizzo dei dati personali per finalità diverse da quelle del Processo.

In generale, le fonti di rischio per i dati personali trattati ai fini del Processo possono essere:

- a) sia fonti interne, operanti - accidentalmente o intenzionalmente - all'interno del Titolare del trattamento, quali dipendenti, utenti e/o amministratori IT del Titolare del trattamento;
- b) o fonti esterne, operanti - accidentalmente o intenzionalmente - al di fuori del Titolare del trattamento, incluse fonti non umane, quali agenti concorrenti, acqua, materiali pericolosi, virus informatici generici, attacchi informatici, ecc.

Alla luce dei rischi sopra elencati, i potenziali impatti sugli interessati che - a seconda della classificazione dei diversi livelli di gravità previsti nell'Allegato 1 alla presente Valutazione d'Impatto sulla Protezione dei Dati - potrebbero verificarsi a seguito del Processo sono i seguenti:

- a) Gli Interessati possono subire conseguenze che potrebbero essere significative e superare con difficoltà reali e gravi secondo il livello di gravità 4, nel caso di
  - Sentimento di violazione della privacy e dei diritti fondamentali (ad esempio, discriminazione);
- b) Gli Interessati possono incorrere in gravi svantaggi, che possono superare nonostante alcune difficoltà secondo il livello di gravità 3, in caso di
  - Problemi relativi alla conoscenza personale o professionale (ad esempio, immagine, reputazione danneggiata, perdita di riconoscimento);
  - Sensazione di invasione della privacy senza danni irreversibili; e
  - Malattie psicologiche minori ma oggettive (diffamazione, reputazione).

Tuttavia, il trattamento derivante dal processo comporta un basso rischio per i diritti e la libertà degli interessati, in quanto il Titolare del trattamento - anche attraverso il CRO - ha messo in atto misure tecniche e organizzative adeguate, come di seguito indicato.

Inoltre, i Soggetti interessati possono trarre beneficio dal processo, in quanto può portare a una migliore comprensione della malattia e delle patologie dei soggetti dello Studio. In particolare, i risultati dello studio possono fornire agli operatori sanitari informazioni importanti per il trattamento futuro dei pazienti affetti da cancro al seno avanzato (ABC).

Di seguito sono elencate le misure tecniche e di sicurezza predisposte sia dallo Sponsor in qualità di Titolare del trattamento che dal CRO in qualità di Responsabile del trattamento per gestire e mitigare tali rischi, al fine di evitare qualsiasi problema di privacy dei dati. **B) Misure volte a mitigare i rischi rilevanti (Sezione 37, paragrafo 7, lettera d) del GDPR)**

### 1. Sicurezza del sito di archiviazione dei dati

I siti in cui sono conservati i dati dello Studio, compresi i centri dati, gli uffici e le strutture di stoccaggio fuori sede, saranno dotati di adeguati controlli di sicurezza fisica.

- Gli spazi del data center sono costantemente monitorati da team di sicurezza in loco e da remoto dal personale del data center mediante webcam di registrazione addestrate in tutti i punti di ingresso/uscita e in numerosi punti di osservazione interni ed esterni e dispongono di controlli per limitare e monitorare l'accesso fisico, richiedendo l'autenticazione multifattoriale o biometrica per entrare.

### 2. Sicurezza della rete

Le reti su cui saranno trasmessi i dati dello Studio saranno protette da accessi o infiltrazioni non autorizzate, sia interne che esterne.

Le misure che saranno adottate per garantire questo includono:

- **Esecuzione di scansioni periodiche delle vulnerabilità esterne e interne** Mantenimento delle difese perimetrali quali firewall, sistemi di prevenzione/rilevamento delle intrusioni e soluzioni di prevenzione della perdita di dati. I firewall e i dispositivi di sicurezza di rete correlati sono rafforzati per soddisfare le best practice di settore basate su standard e mantenuti in uno stato di controllo delle modifiche per garantire che vengano aperte solo le porte minime per le comunicazioni.
- Mantenere le difese interne, come la gestione degli eventi informativi di sicurezza per analizzare i file di log e identificare comportamenti anomali e altre minacce, nonché la segmentazione della rete abbinata al monitoraggio del traffico a livello di pacchetti IP.
- Inventario e controllo delle modifiche dei dispositivi di sicurezza di rete all'interno di un database di gestione della configurazione, compreso il rilevamento e la conferma periodica dei dispositivi hardware.

### 3. Sicurezza della piattaforma

La tecnologia su cui sono archiviati i dati dello Studio, compresi i server, le postazioni di lavoro e i computer portatili, i servizi cloud e altri supporti portatili, sarà protetta dalle minacce conosciute da:

- Garantire l'implementazione e l'aggiornamento di sistemi antivirus o antimalware per tutti i sistemi operativi.

- Garantire che i sistemi operativi dei server e degli endpoint abbiano configurazioni sicure, conformi alle best practice di settore basate su standard e mantenute in uno stato controllato dalle modifiche.
- Garantire l'applicazione tempestiva delle patch di sicurezza raccomandate dal fornitore sia per le applicazioni che per i sistemi operativi, crittografare i dischi rigidi dei laptop e i supporti portatili.
- Assicurarsi che vengano eseguite valutazioni del rischio sui fornitori di cloud utilizzando metodologie accettate dal settore, come Cloud Security Alliance o equivalenti. SSAE16, ISO 27001 o altri report indipendenti forniscono garanzie sui controlli di sicurezza e devono essere valutati quando disponibili.
- Assicurarsi che il software di gestione dei dispositivi mobili sia utilizzato per amministrare i controlli di sicurezza sui dispositivi aziendali in dotazione e sui dispositivi "bring your own".
- Gli endpoint degli utenti (workstation, laptop, dispositivi mobili) sono crittografati e i backup dei dati sono crittografati durante il transito e l'archiviazione nel data center secondario.
- I nuovi sistemi devono prendere in considerazione la crittografia dei dati a riposo, ove opportuno (AES 256, standard SHA 2). I principali sistemi preesistenti sono già stati adattati alla crittografia a riposo o sono in corso di adattamento.
- Nella maggior parte dei sistemi, i sottosistemi di storage sono architettonicamente separati dal livello applicativo.
- Le applicazioni cliniche e diagnostiche sono progettate e testate per garantire controlli tecnici appropriati per la protezione dei dati. I sistemi clinici (GxP) sono convalidati per l'uso previsto, in modo da essere conformi al 21 CFR Part 11 e alle norme FDA di riferimento e alle normative globali analoghe; la convalida offre un ulteriore livello di garanzia dei controlli di sicurezza, compresa la protezione e la tracciabilità dei dati sensibili.
- Utilizzo di procedure di revisione periodica GxP per verificare che i sistemi clinici siano mantenuti in uno stato convalidato per tutta la loro durata.
- Un ciclo di vita di sviluppo del software sicuro e processi di supporto che richiedono una revisione dell'architettura di sicurezza e una scansione delle vulnerabilità per verificare le pratiche di codifica sicure per le applicazioni web (OWASP Top 10).
- Scansione delle vulnerabilità di host e applicazioni che richiede test programmati e/o pre-rilascio per identificare le vulnerabilità. Le vulnerabilità devono essere corrette entro un periodo di tempo definito dalla procedura in base alla criticità.
- Pratiche di gestione delle patch per garantire che le patch di firmware/OS/DB siano applicate in modo tempestivo; i tempi sono definiti proceduralmente in base alla criticità delle patch.

#### 4. Riservatezza dei dati

La riservatezza dei dati dello studio sarà mantenuta proteggendo tali dati ovunque siano conservati e trasmessi. Tali processi e procedure comprendono:

- Mantenere database separati per i diversi tipi di dati e limitare l'accesso a ciascun database a coloro che ne hanno la necessità aziendale.
- L'uso di una crittografia forte e di una pseudonimizzazione accettata dal settore.
- Lo smaltimento sicuro di carta, apparecchiature, supporti e dati.
- La sicurezza dei dati in trasmissione mediante la crittografia.

- Segregazione degli ambienti (ad esempio, gli ambienti di produzione/test/sviluppo sono controllati e mantenuti separati; i dati di produzione non sono ammessi negli ambienti inferiori; le responsabilità di migrazione del codice sono isolate per preservare il controllo delle modifiche).

## 5. Accesso ai dati

L'accesso ai dati dello studio avverrà solo da parte del personale autorizzato del titolare e del responsabile del trattamento attraverso mezzi quali:

- L'uso di nomi utente e password univoci per accedere ai sistemi informatici che ospitano i dati dello studio. Utilizzare più fattori di autenticazione per accedere ai sistemi informatici da remoto.
- Implementare politiche di sicurezza per garantire che le password non siano condivise e che le password dei sistemi siano cambiate periodicamente in linea con le migliori pratiche raccomandate.
- Assicurare che l'accesso ai dati dello studio sia autorizzato e approvato.
- Garantire che l'accesso sia concesso sulla base del minimo privilegio.
- Interrompere l'accesso, se necessario.
- Segregazione dei compiti tra gli utenti (ad esempio, l'uso dell'assegnazione di ruoli di sicurezza per garantire che l'accesso ai dati sia limitato al minimo necessario in base alle responsabilità dei dipendenti; separazione dei ruoli di amministratore/superutente/utente finale).
- Procedure centralizzate di onboarding, cambio di lavoro e offboarding per aggiungere, modificare e rimuovere tempestivamente l'accesso sia alla rete aziendale che alle singole applicazioni.
- Revisione periodica dell'accesso degli utenti per garantire l'efficacia dei processi di aggiunta/modifica/rimozione degli utenti a livello di rete e di applicazione.
- Pratiche di hardening di reti IT, server, database e applicazioni basate su standard che impongono e documentano la configurazione di apparecchiature e software che forniscono accesso ai dati aziendali.

## 6. Elaborazione dei dati

Sia il titolare che il responsabile del trattamento dei dati garantiranno l'applicazione di aspetti appropriati di buone pratiche di sicurezza durante l'elaborazione dei dati dello Studio. Questi processi includono:

- Mantenere e applicare le politiche sulla gestione e la cura sicura dei dati e adottare misure per garantire che tali politiche siano note a tutti i dipendenti attraverso una formazione di sensibilizzazione.
- Assicurare che gli sviluppatori siano formati e aggiornati sulle tecniche di codifica della sicurezza.
- Utilizzo di un database di gestione della configurazione e di processi di gestione della configurazione/modifica per controllare gli ambienti di rete, server, applicazioni e storage.

## 7. Backup dei dati, disaster recovery e continuità aziendale

La continuità dell'accesso ai dati dello studio sarà mantenuta assicurando l'esistenza di pratiche standardizzate di backup e ripristino, adeguatamente protette in transito e a riposo, e supportate da piani di continuità tecnica e organizzativa e da test per garantire la recuperabilità senza compromettere la sicurezza dei dati sensibili. Queste pratiche includono:

- Mantenere pratiche di backup IT standardizzate, utilizzando processi definiti e strumenti configurati per produrre backup incrementali e completi di file share, database, applicazioni e supporti di archiviazione contenenti dati aziendali e dei clienti.
- Garantire che i record di backup siano crittografati in transito e a riposo mentre vengono archiviati in una sede secondaria geograficamente distante e protetta secondo gli stessi standard della sede principale.
- Testare periodicamente la funzione di ripristino per garantire che i file di backup siano e rimangano utilizzabili per tutta la durata della loro conservazione.
- Mantenere piani di disaster recovery IT e sistemi di ripristino adeguati e testare periodicamente tali piani con la relativa documentazione di supporto per garantire che siano adeguati a ripristinare/recuperare/failoverare i sistemi IT in uno stato operativo, con i dati ripristinati allo stato precedente al guasto, entro obiettivi di tempo e punto di ripristino (RTO / RPO) appropriati per la criticità aziendale e la sensibilità dei dati in questione.
- Mantenere piani di continuità aziendale appropriati per le funzioni aziendali critiche e testare periodicamente tali piani con la relativa documentazione di supporto per garantire che tali piani di emergenza siano adeguati per assicurare la continuità dell'attività durante il recupero da una perdita catastrofica delle normali operazioni aziendali.

## **B. MISURE DI SICUREZZA ORGANIZZATIVE**

### 1. Procedure di sicurezza per il personale e per le terze parti

Sia il titolare del trattamento che il responsabile del trattamento garantiranno e manterranno l'integrità del rispettivo personale che accede ai dati dello Studio:

- Esecuzione di controlli sui precedenti dei potenziali dipendenti che avranno accesso ai dati personali.
- Mantenere e applicare le politiche sulla gestione e la cura sicura dei dati e adottare misure per garantire che tali politiche siano note a tutti i dipendenti.
- Fornire una formazione regolare ai dipendenti sulle politiche di privacy e sicurezza e sulla consapevolezza della sicurezza.
- Assicurarsi che i dipendenti e gli appaltatori firmino accordi di riservatezza, o siano comunque soggetti a un obbligo di riservatezza, prima di accedere ai dati dell'esportatore.
- Esaminare eventuali subprocessori che il titolare del trattamento o il responsabile del trattamento utilizzerà, per garantire l'adozione di misure di sicurezza adeguate.
- Assicurarsi che la terza parte aderisca all'insieme minimo di controlli prescritti rispettivamente dalle politiche di sicurezza delle informazioni del titolare o del responsabile del trattamento dei dati.

## 2. Diritti dell'interessato

Sia il titolare del trattamento che il responsabile del trattamento hanno stabilito una serie di procedure per la tutela dei diritti degli interessati al fine di rispettare pienamente le disposizioni degli articoli da 15 a 22 del GDPR.

## 3. Procedure di violazione dei dati

Sia il titolare del trattamento che il responsabile del trattamento hanno stabilito una serie di procedure di sicurezza per la violazione dei dati che comprendono i seguenti elementi:

- Rilevamento: Stabilire i fatti dell'incidente e creare un piano di diagnostica, contenimento e comunicazione con coloro i cui dati sono stati colpiti.
- Contenimento: Limitare la portata della compromissione dei dati.
- Sradicamento: Rimozione di tutti gli aspetti del codice/configurazione ostile, se applicabile.
- Ripristino: Ripristino dei dati e del sistema a uno stato buono conosciuto, senza vulnerabilità.
- Revisione: Valutazione di come evitare incidenti simili in futuro.
- Notifica: Informare le parti interessate della violazione dei dati entro gli obblighi e i tempi previsti dalla legge e dal settore.

Alla luce delle informazioni fornite nel presente documento e tenuto conto delle modalità del processo sopra descritto, il DPO concorda con la valutazione dello Sponsor. Tuttavia, il DPO evidenzia la necessità di attenersi rigorosamente ai limiti in cui i dati personali sono trattati per le finalità e secondo le modalità sopra indicate, rispetto alle quali dà atto che lo Sponsor ha adottato misure di sicurezza, tecniche e organizzative adeguate per ridurre al minimo i rischi derivanti dal trattamento e il possibile impatto sui diritti e sulle libertà degli interessati.

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'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

Data : 30-août-2024 | 14:48:03 CEST

Firma : PIERRE FABRE MEDICAMENT

---

**Pierre-André Poirier**

Responsabile della protezione dei dati

DocuSigned by:  
*Pierre-André Poirier*  
EB9EFD9AD54B461...

## ALLEGATO 1

### Tabella sugli scenari di rischio

Gravità	Descrizione generica degli impatti (diretti o indiretti)	Danni fisici	Danni emergenti	Perdita di guadagno	Discriminazione o stigmatizzazione	Danni all'identità	Danni alla reputazione	Ansia/paura
5	I soggetti interessati possono subire conseguenze significative, o addirittura irreversibili, che non possono superare.	<ul style="list-style-type: none"> <li>- Morte</li> <li>- Lesioni con conseguenze fatali</li> <li>- Invaldità a lungo termine</li> <li>- Perdita permanente dell'integrità fisica</li> </ul>	<ul style="list-style-type: none"> <li>- Rischio finanziario</li> <li>- Debiti sostanziali</li> </ul>	<ul style="list-style-type: none"> <li>- Incapacità di lavorare</li> <li>- Impossibilità di muoversi</li> <li>- Perdita di prove nel contesto di un contenzioso</li> <li>- Perdita di accesso a infrastrutture e vitali (acqua, elettricità)</li> </ul>	<ul style="list-style-type: none"> <li>- Perdita delle relazioni parentali</li> <li>- Sequestro di persona</li> </ul>	<ul style="list-style-type: none"> <li>- Sanzione penale</li> <li>- Cambiamento di status amministrativo e/o perdita di autonomia giuridica (protezione)</li> </ul>	<ul style="list-style-type: none"> <li>- Perdita totale della buona reputazione</li> <li>- Impossibilità di trovare un impiego</li> </ul>	<ul style="list-style-type: none"> <li>- Morte per suicidio</li> <li>- Disturbi psicologici a lungo termine o permanenti</li> </ul>
4	Gli interessati possono andare incontro a conseguenze che potrebbero essere significative e possono trovarsi in difficoltà reali e gravi.	<ul style="list-style-type: none"> <li>- Gravi malattie fisiche che causano danni a lungo termine (ad es. deterioramento della salute a causa di un trattamento improprio o di controindicazioni sottovalutate/ignorate)</li> <li>- Disturbi fisici a lungo termine o permanenti (ad es. a causa del mancato rispetto delle controindicazioni)</li> <li>- Alterazione dell'integrità fisica, ad esempio dopo un'aggressione, un incidente a</li> </ul>	<ul style="list-style-type: none"> <li>- Appropriazione indebita di denaro non compensato</li> <li>- Difficoltà finanziarie non temporanee (ad es. obbligo di prestito)</li> <li>- Danni alla proprietà</li> <li>- Perdita di alloggio</li> <li>- Separazione o divorzio</li> <li>- Perdita finanziaria a seguito di frode (ad esempio dopo un tentativo di phishing)</li> <li>- Bloccato all'estero</li> <li>- Perdita dei dati dei clienti</li> </ul>	<ul style="list-style-type: none"> <li>- Perdita di lavoro</li> <li>- Opportunità mancate, uniche e non ricorrenti (ad esempio, mutui per la casa, rifiuto di studi, tirocini o impieghi, divieto di esami)</li> </ul>	<ul style="list-style-type: none"> <li>- Vittima di ricatto</li> <li>- Bullismo e molestie informatiche</li> <li>- Licenziamento</li> </ul>	<ul style="list-style-type: none"> <li>- Sentimento di violazione della privacy con danni irreversibili</li> <li>- Sensazione di violazione dei diritti fondamentali (ad es. discriminazione, libertà di espressione)</li> </ul>	<ul style="list-style-type: none"> <li>- Gravi danni all'immagine</li> <li>- Danneggiamento della posizione creditizia</li> </ul>	<ul style="list-style-type: none"> <li>- gravi sindromi psicologiche (ad esempio depressione, sviluppo di fobie)</li> <li>- Sensazione di vulnerabilità dopo una chiamata in tribunale</li> </ul>

Gravità	Descrizione generica degli impatti (diretti o indiretti)	Danni fisici	Danni emergenti	Perdita di guadagno	Discriminazione o stigmatizzazione	Danni all'identità	Danni alla reputazione	Ansia/paura
		casa, al lavoro, ecc.						
3	Gli interessati possono trovarsi di fronte a gravi svantaggi, che possono essere superati nonostante alcune difficoltà.	<ul style="list-style-type: none"> <li>- Inabilità temporanea</li> <li>- Mancanza di assistenza che provoca un danno minore ma reale (ad es. disabilità)</li> <li>- Diffamazione che produce ritorsioni fisiche</li> </ul>	<ul style="list-style-type: none"> <li>- Rifiuto di accesso a servizi amministrativi o commerciali</li> <li>- Aumento dei costi (ad es. aumento dei prezzi delle assicurazioni)</li> </ul>	<ul style="list-style-type: none"> <li>- Promozione di carriera persa</li> <li>- Dati obsoleti (ad es. posizioni precedenti)</li> </ul>	<ul style="list-style-type: none"> <li>- Intimidazioni sui social network</li> <li>- Pubblicità online mirata a un aspetto privato che l'individuo desiderava mantenere riservato (ad esempio, pubblicità di gravidanze, trattamenti farmacologici)</li> </ul>	<ul style="list-style-type: none"> <li>- Sensazione di invasione della privacy senza danni irreversibili</li> </ul>	<ul style="list-style-type: none"> <li>- Problemi relativi alla conoscenza personale o professionale (ad es. immagine, reputazione danneggiata, perdita di riconoscimento)</li> <li>- Pubblicità online mirata a un aspetto privato che l'individuo desiderava mantenere riservato (ad esempio, pubblicità di gravidanze, trattamenti farmacologici)</li> </ul>	<ul style="list-style-type: none"> <li>- Diffamazione che produce ritorsioni psicologiche</li> <li>- Rifiuto di continuare a utilizzare i sistemi informativi (avvisi, social network)</li> <li>- Malattie psicologiche e minori ma oggettive (diffamazione, reputazione)</li> </ul>
2	Gli interessati possono trovarsi di fronte ad alcuni inconvenienti, che possono essere superati con poca difficoltà	<ul style="list-style-type: none"> <li>- Lesione superficiale</li> <li>- Minori disturbi fisici (ad es. lieve malattia dovuta al mancato rispetto delle controindicazioni)</li> </ul>	<ul style="list-style-type: none"> <li>- Chiusura di un conto online</li> <li>- Account di servizi online bloccati (ad es. giochi, amministrazioni)</li> </ul>	<ul style="list-style-type: none"> <li>- Nessuna possibilità di stipulare un contratto con il vettore aereo in caso di clonazione della carta</li> </ul>	<ul style="list-style-type: none"> <li>- Scherzi di parenti e amici</li> </ul>	<ul style="list-style-type: none"> <li>- Sentimento di violazione della privacy senza danni reali o oggettivi (ad es. intrusione commerciale)</li> </ul>	<ul style="list-style-type: none"> <li>- Ricezione di messaggi mirati non richiesti che potrebbero danneggiare la reputazione delle parti interessate.</li> </ul>	<ul style="list-style-type: none"> <li>- Periodi temporanei di forte stress</li> <li>- Paura di utilizzare carte di credito e servizi online</li> <li>- Perdita di comfort (ad es. perdita di tempo libero, vacanze)</li> </ul>
1	Gli interessati possono trovarsi di fronte ad alcuni inconvenienti, che possono essere superati senza problemi	<ul style="list-style-type: none"> <li>- Lesione molto lieve</li> <li>- Mancanza di cure adeguate per una persona dipendente (minore, persona protetta)</li> <li>- Mal di testa temporaneo</li> </ul>	<ul style="list-style-type: none"> <li>- Perdita di tempo nel ripetere le formalità o nell'attendere il loro completamento</li> <li>- Ricezione di posta indesiderata (ad es. spam)</li> <li>- Riutilizzo dei dati pubblicati sui</li> </ul>	<ul style="list-style-type: none"> <li>- Perdita di tempo nel ripetere le formalità o nell'attendere il completamento</li> <li>- Mancata possibilità di pagare le utenze a seguito, ad esempio, della clonazione</li> </ul>	<ul style="list-style-type: none"> <li>- Mancanza di rispetto per la libertà di navigazione online a causa del rifiuto di accesso a siti commerciali (ad es. alcolici per età sbagliate)</li> </ul>	<ul style="list-style-type: none"> <li>- Semplice fastidio causato dalle informazioni ricevute o richieste</li> </ul>	<ul style="list-style-type: none"> <li>- Semplice fastidio causato dalle informazioni ricevute o richieste</li> <li>- Trovare informazioni personali di natura comune divulgate in modo non coerente con la realtà</li> </ul>	<ul style="list-style-type: none"> <li>- Paura di perdere il controllo sui propri dati</li> </ul>

Gravità	Descrizione generica degli impatti (diretti o indiretti)	Danni fisici	Danni emergenti	Perdita di guadagno	Discriminazione o stigmatizzazione	Danni all'identità	Danni alla reputazione	Ansia/paura
			siti web per pubblicità mirata (informazioni ai social network, riutilizzo per mailing cartaceo) - Pubblicità mirata per prodotti di consumo comuni	della carta di credito				
0	Nessun danno per gli interessati	Nessun danno fisico per gli interessati	Nessun danno emergente per gli interessati	Nessuna perdita di guadagno per gli interessati	Nessuna discriminazione o stigmatizzazione per gli interessati	Nessun danno all'identità degli interessati	Nessun danno reputazionale per gli interessati	Nessuna ansia/paura per gli interessati