sanofi

Valutazione d'impatto sulla protezione dei dati (Data Privacy Impact Assessment, DPIA)

Titolo del progetto: Rockreal2, uno studio osservazionale retrospettivo

I. Informazioni generali sul trattamento

1. *A quale Attività di Trattamento si riferisce questa DPIA?*

Uso secondario dei dati clinici (ad es. revisioni delle cartelle cliniche)

2. *Fornire una descrizione completa e dettagliata dell'attività di trattamento valutata ai sensi della presente DPIA*

ROCKreal 2 è uno studio globale di revisione retrospettiva non interventistica condotto nel Regno Unito, in Italia e in Spagna. Lo studio utilizza i dati raccolti dalle cartelle cliniche dei pazienti per valutare l'efficacia reale di belumosudil per il trattamento della malattia cronica del trapianto contro l'ospite. I dati presenti nelle cartelle cliniche dei pazienti sono stati inizialmente raccolti dagli operatori sanitari per le cure di routine dei pazienti. Nel Regno Unito, i pazienti sono stati trattati con il prodotto farmaceutico commerciale. In Italia e Spagna, poiché il farmaco non era registrato, i pazienti sono stati trattati attraverso programmi di uso compassionevole. Questa DPIA si concentra specificamente sulla conduzione dello studio in Italia.

3. *Perché i Dati Personali vengono trattati nell'ambito di questa attività e qual è la base giuridica del trattamento?*

I Dati Personali sono trattati per la seguente attività di trattamento: "Condurre studi e sperimentazioni cliniche".

La base giuridica per la raccolta e il trattamento dei Dati Personali dipende dal Soggetto interessato:

- ***Pazienti (partecipanti allo studio):*** Per le persone in vita, la base giuridica è il consenso del paziente (art. 6.1a) e l'art. 9.2 a) GDPR).
  I dati di pazienti deceduti e non rintracciabili potrebbero essere coinvolti nello Studio ai sensi dell'art.110 della Legge italiana sulla privacy, Linee guida emanate il 9 maggio 2024 dal Garante per la protezione dei dati personali e *dalle Regole Deontologiche per la ricerca statistica e scientifica*. La base giuridica in questo caso è l'art. 9.2 j) e gli artt. 36, comma 4 e 89 GDPR, oltre all'art. 110.1 d.lgs. 196/2003. L'inserimento di soggetti deceduti o non rintracciabili è fondamentale per ridurre al minimo i rischi di bias di selezione, come definiti nella Sezione 8.1 del Protocollo.

- ***Operatori sanitari (incluso il personale dello studio):*** La base giuridica è un obbligo legale, poiché Sanofi deve raccogliere alcuni dati di

base sul personale dei centri coinvolto nella conduzione dello studio clinico al fine di rispettare i requisiti normativi.

4. *Quali categorie di Dati Personali vengono raccolte/utilizzate?*

Pazienti (partecipanti allo studio)	***Operatori sanitari (incluso il personale dello studio)***
Dati sanitari Informazioni e rapporti relativi a salute e sicurezza **Dati di identificazione personale** Codice identificativo del paziente nello studio	**Qualifiche educative e professionali** Titoli di studio Qualifiche/certificazioni **Dati relativi all'organizzazione presso cui lavorano gli operatori sanitari** Società/ente Titolo/ruolo professionale **Dati di identificazione personale** Nome, Cognome **Dati di contatto professionali** Indirizzo e-mail professionale Numero di Telefono Professionale

II. Necessità e proporzionalità

1. *Quanto è necessaria questa attività in relazione alla sua finalità?*

L'uso dei Dati Personali è "fondamentale" per il raggiungimento degli obiettivi generali di questo studio e non può essere condotto con dati non personali in quanto è necessaria la tracciabilità.

2. Quanto è proporzionata questa attività in relazione alla sua finalità?

L'attività è "altamente proporzionata": il volume e i tipi di Dati Personali utilizzati sono essenziali per il raggiungimento degli scopi generali di questo Studio e non possono essere modificati senza compromettere tali scopi.

3. In che misura l'uso dei Dati Personali è in linea con le ragionevoli aspettative degli Interessati?

L'uso dei Dati Personali in questo Studio è altamente in linea con le ragionevoli aspettative del Soggetto interessato per le seguenti ragioni.

- ***Pazienti (partecipanti allo studio):***

- I pazienti saranno ricontattati individualmente al fine di ottenere il loro consenso specifico (ad eccezione dei pazienti deceduti);
- Le informazioni generali saranno rese pubbliche sul sito web di Sanofi per consentire alle famiglie dei pazienti deceduti o ai pazienti non rintracciabili di esercitare i propri diritti.

I benefici percepiti da questa attività di trattamento sono lo sviluppo dei prodotti, il benessere pubblico, l'innovazione, la qualità dei prodotti, l'accesso alle risorse, la salute e il benessere, la ricerca scientifica.

- ***Operatori sanitari (incluso il personale dello studio)***

- Sarà fornita un'Informativa Privacy agli sperimentatori principali e ad altri operatori sanitari coinvolti nello studio, come co-sperimentatori, infermieri, ecc.

III. Principi e controlli sulla privacy

1. *Quali misure sono state adottate per garantire che i dati siano trattati in modo equo?*

Lo Studio è stato valutato e approvato da un Comitato Etico indipendente.

2. *Quali misure sono state adottate per garantire che i dati siano trattati in modo trasparente?*

- Per l'Italia, un consenso informato specifico per lo studio sarà fornito a pazienti vivi e raggiungibili al momento dell'ingresso nello studio prima di iniziare la raccolta dei dati per gli scopi dello studio.
- Per i pazienti deceduti e non rintracciabili, i dati saranno raccolti solo dopo il mancato tentativo documentato da parte degli operatori sanitari di raggiungere – a seconda dei casi – le famiglie dei pazienti o i pazienti stessi.

3. *Quali misure sono state adottate per garantire che l'uso dei dati sia conforme a tutti i seguenti requisiti:*
   - *i dati sono stati raccolti e utilizzati solo per finalità specificate, esplicite e legittime?*
   - *I dati non sono ulteriormente trattati in modo incompatibile con tali finalità?*
   - *I dati sono limitati a ciò che è necessario ai fini di questa attività?*

La finalità specifica della raccolta di ciascun Dato Personale è documentato nel protocollo dello studio. Il riutilizzo dei dati dei pazienti è strettamente controllato e disciplinato all'interno della società che promuove lo studio: 1) Le procedure e la formazione globali descrivono le regole da seguire laddove i dati debbano essere riutilizzati. 2) Qualsiasi riutilizzo sarà specificamente valutato da un Responsabile della privacy per la nuova finalità.

4. *Quali misure sono state adottate per garantire che i dati siano pertinenti rispetto alle finalità di questa attività?*

È stato sviluppato, rivisto e approvato un protocollo completo in base ai processi di revisione interna della società che promuove lo studio e tale protocollo è stato approvato da un comitato etico esterno e indipendente.

5. *Quali misure sono state adottate per garantire che i dati siano accurati e, ove necessario, aggiornati?*

La qualità dei dati sarà regolarmente controllata da un punto di vista medico con gli sperimentatori e aggiornata ove necessario.

6. *Quali misure sono state adottate per garantire che i dati siano conservati in una forma che consenta l'identificazione delle persone per non più di quanto sia necessario per le finalità per le quali vengono trattati?*

I dati saranno distrutti dal fornitore di servizi al più tardi 5 anni dopo la fine dello studio.

7. *Come garantite che le persone possano esercitare i loro diritti e controllare i loro Dati Personali?*

Le informative privacy (ad es., moduli di consenso informato specifici e l'informativa privacy disponibile al pubblico) specificano chiaramente i diritti dell'interessato applicabili e il modo in cui le persone possono esercitarli.

8. *Quali misure avete adottato per garantire che i Dati Personali siano trasferiti a terzi in conformità ai requisiti sulla privacy?*

L'Accordo sul trattamento dei dati (Data Processing Agreement, DPA) che incorpora le Clausole contrattuali tipo (Standard Contractual Clauses, SCC) della Commissione UE è già stato stipulato con il fornitore di servizi che gestisce la conduzione dello studio. Poiché il fornitore di servizi opera su base globale, il suo servizio comporta il trattamento e il trasferimento di Dati Personali su base anch'essa globale. I trasferimenti successivi di tale fornitore di servizi sono disciplinati dai Contratti di Trasferimento Infragruppo (IGTA) che incorporano le SCC.

Inoltre il fornitore di servizi è certificato ISO 27001, ISO 27701 e "Cyber Essentials".

IV. Misure tecniche e organizzative

1. *Quali fattori sono stati presi in considerazione nella scelta delle misure di sicurezza?*

I fattori che sono stati considerati per selezionare le misure di sicurezza sono la finalità dell'attività di trattamento dei dati, le misure di sicurezza all'avanguardia inclusa l'opinione del settore e le migliori pratiche, l'ambito e la natura dei dati coinvolti e il contesto in cui il trattamento avrà luogo.

Inoltre, ogni servizio che deve essere fornito dal fornitore di servizi è stato qualificato ai fini della protezione dei Dati Personali.

2. *Quali misure tecniche e organizzative proteggono i dati?*

I Dati Personali del paziente raccolti nell'eCRF sono pseudonimizzati.

Il controllo degli accessi logici è rigorosamente implementato. L'accesso ai Dati Personali è strettamente limitato alle persone che hanno una legittima necessità di conoscerli per svolgere le proprie mansioni lavorative. Tale accesso è concesso solo dopo l'autenticazione tramite un account nominativo, garantendo così la tracciabilità delle operazioni eseguite in conformità con il principio di responsabilità e i requisiti di sicurezza stabiliti dalle normative applicabili in materia di protezione dei dati.

3. *Sono state adottate misure per ripristinare la disponibilità e l'accesso ai dati in modo tempestivo in caso di incidente fisico o tecnico?*

Salvataggio crittografato automatizzato per tutti i sistemi ospitati sull'infrastruttura del fornitore di servizi. I sistemi del fornitore di servizi ospitati su tale infrastruttura sono gestiti e mantenuti dai fornitori di servizi che sono sottoposti a un rigoroso processo di qualificazione, compresa la protezione IT per conformarsi al GDPR e sono soggetti a revisioni e verifiche periodiche.
I dati vengono sottoposti a salvataggio in conformità alla procedura di salvataggio e ripristino dei dati del fornitore di servizi. Tutti i dati elettronici memorizzati sui server presso le strutture dei data center di classe 1 vengono sottoposti a salvataggio completo e accurato dopo ogni giorno lavorativo. Questi salvataggi vengono mantenuti per garantire che i recuperi dei dati siano prontamente disponibili e le registrazioni storiche sono meticolosamente conservate.
Tutti i dati del fornitore di servizi vengono sottoposti a salvataggio per ogni giorno lavorativo, fornendo un cosiddetto "backup snapshot" che può essere visualizzato e recuperato.
Il fornitore di servizi gestisce un salvataggio di 90 giorni, mantenuto su tecnologia a disco. I backup istantanei sono implementati su sistemi di archiviazione configurati per un periodo di 90 giorni di conservazione. Il periodo di 90 giorni comprende 13 snapshot settimanali (che coprono 13 settimane di conservazione) e 7 snapshot giornalieri. Una volta scaduto ciascun periodo di conservazione, viene generato il successivo set di snapshot (orari, giornalieri e settimanali).
La procedura di salvataggio e ripristino del fornitore di servizi assicura:

- il mantenimento di una libreria dei salvataggi per tutti i server di produzione del fornitore di servizi.
- Possibilità di recuperare i file di dati in caso di perdita accidentale.
- I salvataggi sono disponibili per il ripristino di file a breve termine fino a 90 giorni.

Il fornitore di servizi non utilizza nastri di salvataggio. Il salvataggio dei dati avviene tramite una connessione sicura tra i data center in co-ubicazione del fornitore di servizi. Questi server fungono da backup l'uno per l'altro in caso di catastrofe. I salvataggi vengono eseguiti utilizzando snapshot, che vengono

registrati e inviati a una piattaforma di analisi dei log utilizzata per esaminare l'intera cronologia dei salvataggi.
La piattaforma di analisi dei log è configurata per generare allarmi automatici, che vengono attivati in caso di errore nel processo di salvataggio.
Gli errori di salvataggio vengono registrati nella piattaforma ITSM e corretti.

V. Trasferimenti transfrontalieri di dati

1. *I dati saranno trasferiti al di fuori della regione in cui il loro trattamento viene effettuato? Quali misure di salvaguardia sono in atto per i trasferimenti transfrontalieri di dati?*

Il fornitore di servizi opera su base globale e ciò comporta il trattamento e il trasferimento di Dati Personali su base anch'essa globale. Per facilitare i trasferimenti di Dati Personali all'interno del Gruppo del fornitore di servizi, quest'ultimo ha in essere un Accordo di Trasferimento Infragruppo che include le Clausole Contrattuali Tipo. Il fornitore di servizi assicura che tutti i contratti con gli Sponsor e altri fornitori di servizi dispongano di garanzie adeguate per i trasferimenti internazionali (ad es. Clausole contrattuali tipo approvate dalla Commissione UE).

VI. Danni alle persone

1. *Questa attività potrebbe potenzialmente causare uno dei seguenti danni alle persone? Qual è la probabilità che si verifichino potenziali danni? Quali dei controlli identificati contribuiscono ad affrontare il rischio di questi potenziali danni?*

Questa attività potrebbe potenzialmente causare i seguenti danni alle persone:
- inversione non autorizzata del processo di pseudonimizzazione, che potrebbe portare alla reidentificazione degli interessati i cui Dati Personali sono stati precedentemente pseudonimizzati.
- Perdita di riservatezza dei Dati Personali, esponendo potenzialmente le informazioni sensibili ad accesso, divulgazione o diffusione non autorizzati.

Tuttavia, poiché sono in atto numerosi controlli e misure di sicurezza, è improbabile che lo studio possa causare danni alle persone.

VII. Raccomandazione a seguito di revisione del Patient Privacy Officer

Mitigazione dei rischi accettabile

Nel complesso, i rischi per le persone sono "bassi", il che significa che non sono necessarie ulteriori misure, controlli e misure di salvaguardia per mitigare i rischi.