

**Novartis Farma S.p.A.**

Sede legale:

Viale Luigi Sturzo 43

20154 – Milano

Italia

Estratto della valutazione d'impatto sulla protezione dei dati relativa al trattamento dei dati personali nell'ambito degli studi non interventistici (NIS) prospettici e retrospettivi

Introduzione

Il presente documento riassume la valutazione d'impatto sulla protezione dei dati (DPIA) relativa agli studi non interventistici prospettici e retrospettivi condotti da Novartis Farma S.p.a. con sede legale in Milano (MI) in Viale Luigi Sturzo 43 - in qualità di promotore e titolare autonomo del trattamento.

Lo scopo della presente valutazione è verificare e affrontare adeguatamente i rischi connessi al trattamento dei dati personali, compresi i dati relativi alla salute, nel contesto di studi clinici osservazionali, ivi compreso lo scenario in cui il consenso non possa essere utilizzato come base giuridica per il trattamento poiché tali studi possono riguardare pazienti irreperibili (ovvero quando i pazienti non possono essere contattati dal centro di studio utilizzando i mezzi disponibili) o deceduti. Soprattutto nel contesto degli studi retrospettivi non interventistici, vi sono situazioni in cui non è possibile ottenere il consenso al trattamento dei dati personali di un paziente – ad esempio quando, tra la raccolta iniziale dei dati presso un ospedale partecipante e l'inizio di uno studio retrospettivo, un paziente potrebbe essere deceduto o essere diventato irraggiungibile.

Ambito dell'analisi

Questa attività fa parte di un quadro di sviluppo clinico e tecnico più ampio, che comprende diversi studi osservazionali e coinvolge una o più CRO o fornitori di servizi a supporto delle attività operative per conto dello Sponsor.

I centri clinici sono qualificati come titolari del trattamento indipendenti per le informazioni raccolte presso le rispettive sedi, mentre le CRO e gli altri fornitori di servizi agiscono in qualità di responsabili del trattamento per le attività svolte per conto dello Sponsor.

La presente valutazione viene condotta in conformità sia con il Regolamento europeo sulla protezione dei dati sia con i requisiti normativi italiani (incluso l'articolo 35 del GDPR) ed è in linea con le linee guida stabilite dal Garante per la protezione dei dati personali. Ciò è particolarmente rilevante per gli scenari che prevedono l'uso secondario dei dati personali dei pazienti a fini di ricerca, laddove non sia possibile ottenere il consenso perché gli interessati sono irraggiungibili o deceduti.

Descrizione del trattamento

Gli studi osservazionali oggetto della presente valutazione utilizzano informazioni personali provenienti da cartelle cliniche e registri clinici esistenti, originariamente raccolte nel contesto di cure mediche, senza ulteriori interventi sui pazienti. Negli studi retrospettivi vengono utilizzati solo i dati già presenti nelle cartelle cliniche dei pazienti; negli studi prospettici possono essere raccolti anche ulteriori dati clinici nel contesto delle cure in corso.



L'obiettivo di tali studi è quello di produrre evidenze utili per la conoscenza epidemiologica e clinica, in conformità con i principi della ricerca scientifica. Il processo di trattamento di tali dati è rigorosamente disciplinato dal protocollo di studio, che soddisfa i requisiti delle normative di settore specifiche ed è soggetto all'approvazione del Comitato Etico.

Trasparenza e base giuridica

In conformità con il principio di trasparenza e correttezza del trattamento, i pazienti vengono informati tramite ICF in merito alle finalità del trattamento e viene loro richiesto di prestare liberamente il proprio consenso tramite il modulo di consenso informato, in conformità con le normative locali pertinenti e con l' Articolo 14 del GDPR. Gli articoli 6, paragrafo 1, lettera a), e 9, paragrafo 2, lettera a), del GDPR costituiscono la base giuridica pertinente per il trattamento.

Come anticipato in precedenza, il trattamento dei dati personali a fini di studio si basa principalmente sul consenso informato dei pazienti. Nei casi in cui non sia fattibile ottenere il consenso, in particolare negli studi retrospettivi, la base giuridica è costituita dall'art. 6, comma 1, lettera f) e dall'art. 9, comma 2, lettera j) del GDPR, unitamente all' art. 110, comma 1 del Codice della Privacy italiano , che richiede anche un parere favorevole del Comitato Etico competente.

Dati trattati

I dati personali trattati ai fini del NIS comprendono sia categorie comuni di dati personali (ad esempio, informazioni demografiche) sia categorie particolari di dati (informazioni relative alla salute estratte da cartelle cliniche e sistemi sanitari e, se del caso, raccolti dai pazienti). Va sottolineato che, in conformità con la pratica clinica e le normative applicabili in materia di studi clinici, gli identificatori diretti sono conservati separatamente dai set di dati analitici al fine di mitigare il rischio. La pseudonimizzazione viene effettuata assegnando codici al posto degli identificatori diretti, e l'accesso all'elenco di collegamento è strettamente limitato per ridurre il rischio di reidentificazione. Al fine di ridurre ulteriormente il rischio di identificazione la decodifica avviene solo a livello del centro, sostituendo gli identificatori diretti con identificatori dei soggetti. La reidentificazione è possibile solo da parte dei centri stessi nonché da parte del personale autorizzato della CRO per specifiche attività di monitoraggio. Le analisi dei dati vengono condotte esclusivamente su dati codificati. Lo sponsor riceve e analizza solo dati pseudonimizzati.

Terze parti e responsabili del trattamento

Il coinvolgimento di terze parti è regolato da disposizioni contrattuali ben definite e da standard di sicurezza tecnici e organizzativi completi. Le CRO e altri fornitori di servizi, che agiscono in qualità di responsabili del trattamento, operano esclusivamente in conformità alle istruzioni impartite dallo sponsor dello studio. Prima della conclusione di qualsiasi contratto, ogni terza parte viene sottoposta a un rigoroso processo di valutazione dei fornitori che si rinnova ogni tre anni.

Trasferimenti di dati personali

I dati raccolti negli studi possono essere trasferiti ad altre affiliate di Novartis o a terze parti che forniscono servizi a Novartis, che potrebbero avere sede in paesi che non garantiscono lo stesso livello di protezione dei dati richiesto nell'Unione Europea. Per i trasferimenti infragruppo di dati personali , il gruppo Novartis ha adottato le Norme vincolanti d'impresa (Binding Corporate Rules), un sistema di principi, regole e strumenti previsto dalla legislazione europea, al fine di garantire livelli efficaci di protezione dei dati in



relazione ai trasferimenti di dati personali al di fuori del SEE e della Svizzera. In caso di trasferimenti di dati a terzi, i dati personali vengono trasferiti sulla base delle Clausole contrattuali standard approvate dalla Commissione europea.

Analisi dei rischi e misure di mitigazione

L'analisi ha preso in esame aspetti relativi all'utilizzo dei dati personali, con particolare riferimento alla mancanza di consenso per ulteriori trattamenti.

- Rischio di potenziali danni legati all'utilizzo dei dati dei pazienti:** il rischio è considerato basso. Tutti i dati dei pazienti utilizzati in questo studio sono codificati, pertanto non è possibile identificare direttamente le persone. Qualsiasi potenziale danno derivante dall'utilizzo di questi dati potrebbe verificarsi qualora le informazioni sui pazienti raccolte durante il trattamento venissero utilizzate per altri scopi senza il loro consenso. Questo rischio viene affrontato garantendo che: a) l'utilizzo dei dati per lo studio sia conforme alle leggi vigenti in materia di privacy; b) la necessità e la possibilità di ottenere il consenso siano accuratamente verificate; c) sia ottenuta l'approvazione del Comitato Etico quando richiesto.
Le misure organizzative limitano l'accesso ai dati alle sole persone autorizzate in base al principio della «*need to know*», in linea con le procedure e i regolamenti standard dell'azienda Sponsor. Qualora non fosse possibile ottenere il consenso (ad esempio nel caso di pazienti deceduti), verrà richiesta l'approvazione del Comitato Etico per l'utilizzo dei loro dati ai fini dello studio.
- Rischio di perdita dei dati:** il rischio è valutato come basso. Questo studio utilizza, per la parte retrospettiva, dati secondari già raccolti e archiviati nelle cartelle cliniche; di conseguenza, eventuali dati persi durante lo studio possono essere ripristinati dai sistemi di origine. Per la parte prospettica, altresì, i dati sono presenti sia nelle cartelle cliniche del centro che nella eCRF dello studio. Pertanto oltre a non incidere sulla conoscenza dello stato di salute del paziente, possono essere ripristinati. Inoltre, l'implementazione di backup regolari dei dati e di solidi meccanismi di controllo degli accessi riduce ulteriormente la probabilità e l'impatto della perdita dei dati.
- Rischio di alterazione dei dati:** il rischio è considerato basso. Questo studio utilizza esclusivamente copie delle cartelle cliniche esistenti, che non possono essere modificate o alterate da alcuna azione intrapresa durante la ricerca. Le analisi vengono condotte su queste copie, seguendo il protocollo dello studio, e i dati vengono pseudonimizzati per rispettare il principio di minimizzazione.
- Rischio di divulgazione non autorizzata:** il rischio è valutato come basso. Tali rischi vengono affrontati mediante la pseudonimizzazione dei dati – sostituendo gli identificatori diretti con ID dei soggetti – e l'implementazione di solide misure di sicurezza durante l'intero trattamento dei dati. I protocolli di sicurezza includono, tra l'altro: (i) l'applicazione di rigide politiche di accesso basate sul principio del «*need-to-know*», (ii) l'assegnazione di identificatori univoci a tutti gli utenti del sistema e (iii) l'applicazione di procedure comprensive di sistemi di controllo degli accessi.
Il rischio associato all'utilizzo di fornitori di servizi terzi è mitigato (i) selezionando responsabili del trattamento che offrano solide garanzie in merito al rispetto degli accordi contrattuali e all'attuazione delle misure di sicurezza richieste, (ii) incorporando nell'accordo meccanismi di supervisione, verifica e audit per monitorare le attività di trattamento da parte di terzi, e (iii) conducendo audit periodici dei responsabili del trattamento per confermare l'adesione ai termini stabiliti. Inoltre, tutti i dati forniti ai responsabili del trattamento sono pseudonimizzati e l'accesso



è gestito tramite autorizzazioni basate sui ruoli, riducendo così in modo sostanziale la probabilità di accessi non autorizzati o di uso improprio.

Conclusioni

Gli studi non interventistici riguardano, per loro natura, l'uso secondario di dati già presenti nelle cartelle cliniche dei pazienti e raccolti in precedenza per scopi diversi (ad esempio nel corso del normale trattamento del paziente). Lo studio utilizza dati raccolti e codificati dai centri tramite gli identificativi dei pazienti. Vengono analizzati solo i dati codificati. In conformità con il principio di minimizzazione dei dati, vengono raccolte solo le informazioni essenziali indicate nel protocollo dello studio. Il protocollo viene quindi sottoposto al comitato etico competente per la revisione e l'approvazione.

La valutazione ha preso in considerazione diversi scenari di rischio; tuttavia, ciascuno di essi è sufficientemente mitigato da adeguati controlli attuati tramite clausole contrattuali con terze parti e con i responsabili del trattamento (rispettivamente centri di studio e fornitori di servizi terzi) e da misure di sicurezza tecniche e organizzative (ad esempio, pseudonimizzazione dei dati trattati, gestione appropriata degli accessi).

Ove applicabile, viene sempre data priorità all'ottenimento del consenso informato da parte dei partecipanti allo studio (pazienti). In situazioni che coinvolgono pazienti deceduti o quando non è possibile ottenere il consenso, è consultato il Comitato Etico per ottenere l'approvazione all'utilizzo dei dati di tali pazienti nello studio. Inoltre, la presente sintesi della DPIA è pubblicata e ne sarà data comunicazione al Garante per la protezione dei dati personali. Tale valutazione è stata effettuata con la certezza che, a seguito della stessa, non sia stato individuato alcun danno potenziale o effettivo.

In conclusione, il trattamento dei dati viene effettuato nel rispetto dei principi di liceità, trasparenza, minimizzazione dei dati, integrità e riservatezza. Il rischio residuo associato al trattamento dei dati personali degli individui è valutato come basso.

La presente sintesi della DPIA è stata esaminata e approvata dal Responsabile della protezione dei dati di Novartis contattabile all'indirizzo global.privacy_office@novartis.com.


ERC Data Privacy, Digital& AI Compliance Head


Local Clinical Operation Head

