

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

INFORMAZIONI SULLA DPIA

DPIA

Ricerca scientifica – campioni biologici

Redattore

Dondi Alessandra

Revisore

Giuseppe Rossi

Validatore

Andrés J. M. Ferreri

Data di creazione

21 gennaio 2022

DPO

La Torre Cathy

Parere DPO

Il parere del DPO è favorevole

Motivazione DPO

Le misure di sicurezza adottate per la protezione dei dati di ricerca scientifica sono al momento adeguate; è comunque opportuno procedere al rinnovo di DPIA a stretto giro per continuare a controllare l'adeguatezza delle misure di sicurezza.

CONTESTO

Panoramica

Descrizione del trattamento preso in considerazione

Dati relativi a stato di salute, sesso, dati genetici, origini etniche, carte sanitarie, vita sessuale per finalità di ricerca scientifica

Finalità associate al trattamento

Ricerche biomediche; Ricerche epidemiologiche

Categorie di soggetti interessati dal trattamento

Pazienti

Titolari del trattamento

Fondazione Italiana Linfomi Onlus

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Responsabili del trattamento

I responsabili del trattamento sono i Laboratori di analisi

Norme applicabili al trattamento

GDPR 2016/679, Codice Privacy e s.m.i.

Valutazione: Accettabile

Dati, processi e asset di supporto

Descrizione dei dati trattati

Dati genetici; Stato di salute; Origini etniche; Carte sanitarie; Vita sessuale; Sesso m/f

Durata di archiviazione dei dati

I documenti relativi allo studio, inclusi i dati del paziente raccolti presso il centro, saranno conservati per un massimo di 10 anni dalla conclusione dello studio.

Categorie di destinatari dei dati

Enti pubblici non economici

Destinatari identificati dei dati

Comitati Etici; Autorità sanitarie; Laboratori medici

Soggetti autorizzati al trattamento

Staff autorizzato alla gestione dello studio; enti regolatori in caso di ispezione.

Ciclo di vita dei dati

I dati vengono raccolti, nei Centri di sperimentazione, dalla firma del consenso del paziente per tutta la durata dello studio e vengono conservati per un periodo massimo di dieci anni dalla conclusione dello studio stesso. Questa procedura vale sia per i dati dei pazienti ancora in vita che per quelli dei pazienti defunti. Il centro inserisce i dati su un Case Report Form (Modulo di raccolta dati clinici, CRF) elettronico. Tutti i dati raccolti sono codificati e vengono trasmessi alla Fondazione Italiana Linfomi Onlus. I dati vengono elaborati statisticamente e pubblicati in forma

Elenco degli assetti di supporto

Database FIL dello Studio; CRF; TMF

Descrizione degli asset di supporto

I dati dei pazienti sono raccolti tramite CRF elettroniche (portali REDCap) e tramite trial master file (TMF) dello studio cartaceo ed elettronico

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Le finalità del trattamento sono esplicite, specifiche e legittime?

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Le finalità del trattamento sono esplicitate nel Modulo Privacy paziente "INFORMATIVA E MANIFESTAZIONE DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ARTICOLO 13 REGOLAMENTO UE SULLA PRIVACY" e riguardano ricerche biomediche ed epidemiologiche.

Valutazione: Accettabile

Quali sono i principi di liceità che rendono il trattamento legittimo?

Le basi legali del trattamento dei dati nell'ambito delle sperimentazioni cliniche sono: Norma Unione Europea (GDPR 2016/679), Norme di Buona Pratica Clinica dell'International Conference on Harmonization (ICH- Guidelines), Norme in materia di sperimentazioni cliniche. Inoltre, per i dati dei pazienti defunti le basi giuridiche sono l'art. 110 del Codice Privacy e s.m.i. e l'art. 36 del GDPR.

Valutazione: Accettabile

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

I dati raccolti sono adeguati al raggiungimento degli obiettivi primari e secondari dello studio clinico indicati nel protocollo valutato dai Comitati Etici dei centri partecipanti. La FIL applica il principio della minimizzazione nella raccolta dei dati. Questo processo di minimizzazione viene applicato già a partire dalla fase iniziale di stesura del protocollo di studio.

Valutazione: Accettabile

I dati sono accurati e mantenuti aggiornati?

La completezza, la congruità e l'accuratezza dei dati viene verificata in occasione di controlli periodici eseguiti con tempistiche definite nei piani di monitoraggio e secondo procedure standard specifiche delle Aree coinvolte nel processo di raccolta e monitoraggio dati.

Valutazione: Accettabile

Qual è la durata della conservazione dei dati?

Il trattamento dei dati dei pazienti potrà essere effettuato sia con strumenti elettronici sia su supporti (secondo i casi) di tipo cartaceo o elettronico e ciò potrà avvenire per il tempo necessario a conseguire gli scopi per cui le informazioni personali sono state raccolte (la durata dello studio – 36 mesi). Successivamente, i dati personali in formato pseudonimizzato saranno conservati per un massimo di dieci anni dal termine dello studio previo consenso dei pazienti reperibili. Tale indicazione di conservazione sarà comunicata anche ai responsabili del trattamento.

Valutazione: Accettabile

Misure di protezione dei diritti degli interessati

I soggetti interessati come sono informati del trattamento?

Ogni paziente riceve un Foglio Informativo dettagliato sullo studio clinico e su altri sotto-studi se presenti oltre che sul trattamento dei dati. Per i pazienti deceduti o non rintracciabili sarà resa pubblica l'informativa sul trattamento dei dati personali.

Valutazione: Accettabile

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Come si ottiene il consenso dei soggetti interessati?

Il paziente, sottoscrivendo il modulo per il trattamento dei dati acconsente al trattamento stesso, compreso quello dei dati particolari quali ad esempio lo stato di salute, per gli scopi della ricerca nei limiti e con le modalità indicate nell'informativa. Per i pazienti deceduti il trattamento avviene sulla base degli artt. 110 del Codice Privacy e s.m.i e dell'art. 36 del Reg. UE 2016/679.

Valutazione: Accettabile

I soggetti interessati come esercitano i loro diritti di accesso e alla portabilità dei dati?

Sui moduli forniti al paziente sono indicati diritti e modalità per esercitare gli stessi. L'esercizio dei diritti può avere luogo rivolgendo la relativa richiesta al Titolare dei dati ai recapiti indicati nei moduli stessi, anche per il tramite di uno degli Incaricati del trattamento o mediante raccomandata, telefax o posta elettronica o altro mezzo idoneo individuato dal "Garante per la protezione dei dati personali". Fermo restando il diritto dell'interessato di proporre reclamo all'autorità Garante per la protezione dei dati personali (www.garanteprivacy.it).

Valutazione: Accettabile

I soggetti interessati come esercitano i loro diritti alla rettifica e alla cancellazione dei dati?

Sui moduli forniti al paziente sono indicati diritti e modalità per esercitare gli stessi. L'esercizio dei diritti può avere luogo rivolgendo la relativa richiesta al Titolare dei dati ai recapiti indicati nei moduli stessi, anche per il tramite di uno degli Incaricati del trattamento o mediante raccomandata, telefax o posta elettronica o altro mezzo idoneo individuato dal "Garante per la protezione dei dati personali". Fermo restando il diritto dell'interessato di proporre reclamo all'autorità Garante per la protezione dei dati personali (www.garanteprivacy.it).

Valutazione: Accettabile

I soggetti interessati come esercitano i loro diritti di limitazione e opposizione al trattamento?

Sui moduli forniti al paziente sono indicati diritti e modalità per esercitare gli stessi. L'esercizio dei diritti può avere luogo rivolgendo la relativa richiesta al Titolare dei dati ai recapiti indicati nei moduli stessi, anche per il tramite di uno degli Incaricati del trattamento o mediante raccomandata, telefax o posta elettronica o altro mezzo idoneo individuato dal "Garante per la protezione dei dati personali". Fermo restando il diritto dell'interessato di proporre reclamo all'autorità Garante per la protezione dei dati personali (www.garanteprivacy.it).

Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?

Ciascun professionista esterno coinvolto nel trattamento dei dati è stato incaricato come Responsabile esterno del trattamento.

Valutazione: Accettabile

I dati sono adeguatamente protetti nel caso di trasferimento al di fuori dell'Unione Europea?

I dati potranno essere trasmessi a soggetti terzi o società esterne, sempre in forma pseudonimizzata (codificata in modo da non poterla identificare) in Paesi appartenenti all'UE che applicano il Regolamento generale sulla protezione dei dati (GDPR) o in paesi al di fuori dell'UE che garantiscono un adeguato livello di protezione dei dati codificati. Tra questi soggetti vi sono fornitori di servizi connessi alle finalità del trattamento: server schede di raccolta dati e archivi

Valutazione: Accettabile

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

RISCHI

Misure esistenti o pianificate

Pseudonimizzazione

I dati sono raccolti all'origine in forma pseudonimizzata: il centro al momento dell'arruolamento di un nuovo paziente accede alla piattaforma raccolta dati che genera automaticamente un codice univoco che verrà utilizzato dal centro per qualsiasi comunicazione riguardante il paziente stesso.

Valutazione: Accettabile

Controllo dell'accesso logico

L'accesso a informazioni e funzioni di sistemi applicativi è stato limitato secondo le politiche di controllo degli accessi. Un processo di gestione formale garantisce l'assegnazione di informazioni segrete di autenticazione. Soltanto gli utenti autorizzati ricevono l'accesso al portale per raccolta dei dati degli studi clinici. Nello specifico l'utente deve autenticarsi ai portali specifici di raccolta dati: <https://redcap.filinf.it> e <https://openclinica.filinf.it> con username e password che scade ogni 90 giorni e di lunghezza minima di 12 caratteri. L'accesso ai portali è subordinato al completamento della procedura di attivazione del centro clinico nello specifico protocollo di studio. Se l'utente non è più autorizzato ad accedere ai dati si procede con l'aggiornamento dei diritti di accesso in seguito alla comunicazione da parte del centro o successivamente ai monitoraggi dei siti di ricerca con apposita verifica dei log di accesso in relazione alla funzione di compilazione eCRF. I responsabili del monitoraggio degli studi riesaminano ad intervalli regolari i diritti di accesso degli utenti. Sono stati limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato in modo tale che soltanto gli utenti dell'area dati e gli amministratori di sistema posso attivare la procedura di abilitazione utente sui portali di raccolta dati. I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni sono stati rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione. Le piattaforme di raccolta dati registrano il log degli accessi in maniera tale da avere un report di controllo degli eventi di autenticazione.

Valutazione: Accettabile

Tracciabilità (registrazione degli eventi)

La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni è effettuata, mantenuta e riesaminata periodicamente. Le strutture per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati. Le attività degli amministratori e degli operatori di sistema sono sottoposte a log, e questi sono protetti e riesaminati periodicamente.

Valutazione: Accettabile

Protezione piattaforme

Le piattaforme utilizzano dei controlli crittografici per la protezione delle informazioni attraverso connessione TLS tramite certificato HTTPS. Le chiavi di accesso sono custodite in maniera sicura e protette da password dagli amministratori di sistema. Le password degli utenti sono crittografate in fase di salvataggio. I webserver sono protetti attraverso sistemi di identificazione e prevenzione degli accessi non autorizzati.

Valutazione: Accettabile

Backup dei dati

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Il backup viene effettuato in maniera giornaliera. La procedura prevede 2 fasi: Fase 1: Creazione dei file, ovvero creazione della cartella giornaliera, effettuazione del dump (copia immagine del DB) e invio a server SFTP su cloud tramite connessione crittografata. Fase 2: Copia dei file sul disco di backup, copia delle cartelle utente, copia incrementale della cartella contenente i file di dump.

Valutazione: Accettabile

Rischio di accesso illegittimo ai dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si manifestasse?

Perdita dati

Quali sono le principali vulnerabilità che possono condurre al rischio?

Errata attribuzione dei diritti di accesso

Quali sono le minacce?

Errore nello svolgimento di mansioni

Quali tra le misure identificate contribuiscono a gestire il rischio?

Controllo dell'accesso logico

Stima della gravità del rischio

Medio

Il rischio è legato alla qualità dei dati della ricerca ma non lede i diritti del paziente in quanto i dati sono in formato pseudonimizzato.

Stima della probabilità del rischio

Mai verificatosi ma possibile

L'evento non si è mai verificato ma non è possibile escluderlo per il futuro.

Valutazione: Accettabile

Rischio di modifica non desiderata dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si manifestasse?

Errati risultati della ricerca

Quali sono le principali vulnerabilità che possono condurre al rischio?

Attività di monitoraggio

Quali sono le minacce?

Carenza di personale

Quali tra le misure identificate contribuiscono a gestire il rischio?

Tracciabilità (registrazione degli eventi)

Stima della gravità del rischio

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Medio

Il rischio è legato alla qualità dei dati della ricerca ma non lede i diritti del paziente

Stima della probabilità del rischio

Periodico

Sono stati riscontrati nel corso di alcuni controlli mirati errori nella compilazione delle schede CRF da parte dei centri clinici.

Valutazione: Accettabile

Rischio di perdita dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si manifestasse?

Violazione dei diritti dei pazienti

Quali sono le principali vulnerabilità che possono condurre al rischio?

Abbandono della postazione senza effettuare la disconnessione dal sistema

Quali sono le minacce?

Furto di apparecchiature o documenti

Quali tra le misure identificate contribuiscono a gestire il rischio?

Gestione del personale

Stima della gravità del rischio

Alto

Anche se i dati sono raccolti in forma pseudonimizzata un accesso illecito potrebbe comportare un rischio per i diritti del paziente

Stima della probabilità del rischio

Mai verificatosi ma possibile

L'evento non si è mai verificato ma non è possibile escluderlo per il futuro.

Valutazione: Accettabile

Valutazione d'impatto sulla protezione dei dati (DPIA)

(art 35 GDPR 2016/679)

Io sottoscritto **Andrés J. M. Ferreri**, in qualità di soggetto validatore della DPIA collegata al trattamento **Ricerca scientifica**, dopo aver esaminato l'intera valutazione di impatto effettuata:

- Confermo che la descrizione del contesto del trattamento è coerente con la realtà
- Confermo di aver preso nota dei rischi esistenti in base alle misure pianificate o esistenti
- Approvo le misure correttive indicate
- Mi impegno ad attuare quanto prima le misure correttive indicate

Firma del Validatore della DPIA

Andrés J. M. Ferreri

A handwritten signature in black ink, consisting of a large, stylized 'A' followed by 'J. M. Ferreri' in a cursive script.