VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI

Informazioni Generali sullo Studio

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

Identificativi dello Studio

A CURA DEL RICERCATORE

Titolare del Trattamento: Ospedale San Raffaele

Codice di Protocollo: Chewbacca

Titolo dello Studio: Titolo in Italiano: personalizzazione del trattamento adottivo di cellule per tumori solidi: verso una nuova opzione terapeutica su misura per il

paziente Titolo in inglese: Personalizing Adoptive Cell Transfer for solid tumors: towards a new patient-tailored treatment optionzzazione

Sperimentatore Principale: Prof. Novellis Pierluigi ; Dr.ssa Chiara Cattaneo

Unità: Chirurgia Toracica

Data di Compilazione: 04/05/2026

Sinossi dello Studio:

si allega la sinossi e la lettera di trasmissione dell'emendamento, protocollo, consenso informato , privacy che segue il consenso e informativa per legge.

Avevamo già inoltrato la richiesta di DPIA che era stata accettata pochi mesi fa. Abbiamo dovuto modificare la documentazione protocollo, consensi, privacy a seguito dell'inserimento come Co-Promotore IRCCS Istituto Clinico Humanitas.

Modalità di Raccolta

Modalità di Raccolta Dati:

- da cartelle cliniche/documentazione sanitaria

Se Altro, specificare la modalità di raccolta:

Trattamento dei dati: Cartaceo

Se Altro, specificare tipologia di raccolta:

Categorie di Persone Interessate:

- Pazienti

Se Altro, specificare la categoria di persone:

Categorie di Dati Trattati:

- dati sulla salute fisica o psichica

Se Altro, specificare la categoria di dati trattati:

Dati Condivisi con Altri: SI

Ambiti di Comunicazione con altri: Altri centri

Dati Trasferiti all'Estero: NO

Paesi Estero Coinvolti:

Misure di Protezione dei Dati

Dati Identificativi Conservati: SI

Se SI specificare le ragioni sottostanti a tale esigenza: Per uso scientifico per eventuale controllo dei dati dello studio.

Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca

Misure di Pseudonimizzazione: Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti

Se Altro, Specificare la procedura utilizzata per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca:

Misure di Anonimizzazione: I dati personali sono sostituti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario

Se si utilizzano tecniche diverse dalla crittografia o utilizzo di codici univoci, specifica in dettaglio:

PRINCIPI, FINALITA' E BASI GIURIDICHE

Necessità e proporzionalità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

☑ Sì ☐ No

Motivare la risposta:

1. **Specificità degli scopi:** Gli scopi del trattamento sono chiaramente e analiticamente definiti all'interno del protocollo. In relazione agli obiettivi dello studio, il trattamento è legato esclusivamente alla ricerca così come dettagliatamente descritta e non a ulteriori scopi; pertanto, le finalità risultano circoscritte al contesto descritto. L'uso dei dati è confinato a uno scopo ben definito e non a fini generici o non correlati.

Nella parte prospettica dello studio, oltre all'analisi di dati raccolti retrospettivamente, il protocollo prevede la raccolta di nuovi dati direttamente dagli interessati nel corso del follow-up clinico, attraverso visite di controllo programmate. La raccolta avviene nel rispetto delle finalità di ricerca dichiarate, senza estensioni indebite del trattamento.

2. **Esplicitazione degli scopi:** Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Gli stessi sono funzionali a raccogliere evidenze scientifiche, migliorare la comprensione delle patologie/trattamenti descritti, e i relativi dati saranno trattati in modo proporzionale all'obiettivo.
   Per la parte prospettica dello studio la raccolta di dati in tempo reale permette di ottenere informazioni aggiornate, migliorando l'accuratezza delle analisi. Gli scopi della raccolta prospettica sono esplicitati nel modulo di consenso informato fornito ai partecipanti al momento dell'arruolamento, garantendo trasparenza e chiarezza sulle finalità del trattamento.
3. **Legittimità degli scopi:** Per quanto riguarda la legittimità, lo studio osservazionale deve rispettare i requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento è finalizzato alla ricerca, e non a scopi commerciali, rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR, che consente il trattamento di dati sanitari per motivi di ricerca scientifica, soggetto all'adozione di adeguate misure di sicurezza e minimizzazione dei dati.
   Nella parte prospettica dello studio viene richiesto un consenso informato specifico agli interessati, conforme ai requisiti normativi, che autorizza l'uso dei nuovi dati raccolti nel corso dello studio. L'eventuale revoca del consenso comporterà l'interruzione della raccolta di dati prospettici, senza pregiudicare l'uso dei dati già raccolti nel rispetto delle disposizioni etiche e regolatorie.
4. **Proporzionalità e necessità:** Riguardo a proporzionalità e necessità, i dati trattati sono strettamente necessari a raggiungere gli obiettivi dello studio. Nel contesto di uno studio retrospettivo, ciò implica l'uso di dati già raccolti in precedenza, riducendo al minimo il rischio di interferenze non necessarie con la protezione dei dati degli interessati. L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.
   Per la parte prospettica, la raccolta avviene nel rispetto del principio di minimizzazione, limitandosi ai dati essenziali per l'analisi scientifica e garantendo adeguate misure di sicurezza (es. pseudonimizzazione, accesso controllato ai dati).

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

☑ Sì ☐ No

Motivare la risposta: La valutazione circa la pertinenza, limitazione e necessità in relazione alle finalità dello studio in oggetto è basata sul principio di minimizzazione dei dati (art. 5(1)(c) del GDPR):

1. **Adeguatezza dei dati:** I dati raccolti sono appropriati per raggiungere le finalità dello studio. Nello studio osservazionale retrospettivo descritto, significa che i dati selezionati oggetto di trattamento sono strettamente necessari per rispondere ai quesiti oggetto della ricerca e alle ipotesi formulate nel protocollo. I dati trattati sono scelti in base alla loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio. Per la parte prospettica, la raccolta di nuovi dati avviene in base a criteri predefiniti che garantiscono l'adeguatezza rispetto agli obiettivi della ricerca, senza raccogliere informazioni non pertinenti. I dati raccolti in tempo reale sono mirati a completare il set informativo necessario per rispondere agli endpoints dello studio.
2. **Pertinenza dei dati:** Nel contesto retrospettivo, vengono trattati solo i dati rilevanti rispetto agli obiettivi scientifici, evitando l'inclusione di informazioni non essenziali. Nel contesto prospettico, la selezione dei dati da raccogliere è basata sulla loro importanza rispetto agli outcome di ricerca. I dati raccolti durante il follow-up dei pazienti sono definiti a priori nel protocollo e devono rispondere a criteri chiari di pertinenza. In entrambi i casi, non vengono trattati dati che non abbiano una connessione chiara con le finalità dichiarate, limitando il trattamento alle informazioni essenziali per la validità scientifica dello studio.
3. **Limitazione dei dati (minimizzazione):** Il protocollo prevede la raccolta dei soli dati strettamente necessari per conseguire le finalità dello studio. Per lo studio retrospettivo, si utilizzano solo i dati pregressi indispensabili, selezionando accuratamente quelli rilevanti ed evitando informazioni ridondanti. Per lo studio prospettico, la raccolta è limitata a informazioni specifiche e necessarie per il monitoraggio nel tempo, escludendo dati eccessivi o non funzionali alla ricerca. In entrambi i casi, vengono adottate misure tecniche e organizzative per ridurre l'impatto sulla privacy degli interessati:
    - Pseudonimizzazione dei dati raccolti per limitare l'identificabilità diretta.
    - Controllo degli accessi ai dataset per prevenire trattamenti non autorizzati.

- Meccanismi di verifica periodica per valutare la necessità della raccolta dati prospettica e, se necessario, limitare o interrompere la raccolta di informazioni non più essenziali.

4. **Necessità dei dati:** Relativamente al principio di necessità, lo studio non potrebbe essere condotto correttamente senza il trattamento dei dati previsti dal protocollo. Ogni categoria di dato trattato è necessaria per fornire risultati significativi e validi scientificamente. La raccolta di ulteriori dati fuori protocollo non essenziali non sarebbe in alcun modo giustificata. Per la parte prospettica, la raccolta di nuovi dati è essenziale per monitorare l'evoluzione delle condizioni cliniche e valutare gli outcome nel tempo, garantendo la robustezza dei risultati scientifici. Pertanto, è possibile considerare i dati adeguati perché appropriati allo scopo dello studio, pertinenti perché direttamente legati alle finalità dichiarate e limitati in quanto raccolti solo nella misura strettamente necessaria per la ricerca, nel rispetto del principio di minimizzazione dei dati previsto dal GDPR.

Integrità ed esattezza

I dati sono esatti e aggiornati?

☑ Sì ☐ No

Motivare la risposta:

1. **Esattezza dei dati:** Lo studio osservazionale retrospettivo si basa su dati già esistenti, raccolti in precedenza per finalità cliniche. Poiché originariamente utilizzati per diagnosi e trattamenti medici, i dati sono stati raccolti e registrati con un alto livello di accuratezza e precisione, in quanto necessari per garantire la cura dei pazienti. Le fonti dei dati, quali ad esempio cartelle cliniche, referti o database ospedalieri, sono dunque affidabili in quanto strumentali al corretto trattamento del paziente, il che assicura una raccolta attenta e precisa delle informazioni.
   Per la parte prospettica, i dati vengono raccolti in tempo reale secondo procedure standardizzate che ne garantiscono la qualità. La raccolta avviene seguendo criteri metodologici stabiliti nel protocollo dello studio, riducendo al minimo errori e discrepanze. In entrambi i casi, i dati trattati sono scelti in base alla loro qualità e rilevanza per la ricerca, evitando informazioni incomplete o imprecise.
2. **Validazione delle fonti dei dati:** Per i dati retrospettivi, le fonti sono istituzionalmente validate (es. cartelle cliniche, referti diagnostici, database ospedalieri) e soggette a controlli di qualità, garantendo la precisione delle informazioni.

Per i dati prospettici, la raccolta è effettuata secondo procedure predefinite con controlli immediati sulla correttezza dell'inserimento dei dati, come il double data entry o l'uso di strumenti elettronici certificati (eCRF – electronic Case Report Form).

3. **Controlli e verifiche incrociate:** Per garantire l'esattezza dei dati raccolti, vengono applicate le seguenti metodologie di controllo, adattate a ciascuna fase dello studio:
   - Retrospettivo: Revisione e pulizia dei dati storici, con strumenti di data cleaning e analisi statistica per identificare anomalie. - Prospettico: Controllo immediato della qualità dei dati in fase di raccolta, con l'applicazione di procedure come audit trail, query management, risk-based monitoring e source data verification (SDV) per ridurre gli errori di trascrizione o inserimento.
4. **Aggiornamento dei dati:**
   - Nel contesto retrospettivo, i dati utilizzati sono pertinenti per il periodo temporale dello studio e riflettono fedelmente la condizione clinica del paziente in quel determinato momento. Non necessitano di aggiornamenti in senso tradizionale, ma devono mantenere la loro coerenza con il periodo di riferimento. - Nel contesto prospettico, invece, i dati sono raccolti e aggiornati progressivamente nel tempo, in base al follow-up previsto. Eventuali nuove informazioni rilevanti per lo studio vengono integrate, garantendo che i dati siano sempre attuali rispetto agli obiettivi della ricerca.
5. **Misure di mitigazione del rischio:** Esclusivamente i dati accurati e affidabili vengano inclusi nelle analisi finali: lo studio adotta misure di mitigazione come l'esclusione di record non completi o poco chiari. Pertanto i dati trattati nello studio sono esatti perché raccolti da fonti affidabili e soggette a controlli di qualità, accurati nel contesto clinico originario e aggiornati rispetto al periodo storico di interesse. Inoltre, lo studio prevede misure per verificare la correttezza dei dati e garantire che qualsiasi eventuale errore venga identificato e corretto.

Durata di Conservazione dei Dati

Per quanto tempo verranno conservati i dati raccolti? 7 ANNI

Decorsa la data di conservazione i dati verranno: Anonimizzati completamente

Se Altro, specificare il destino dei dati:

Basi Giuridiche

Basi Giuridiche del Trattamento: art. 110, co. 1 primo periodo Codice Privacy

Motivi per cui non è possibile fornire l'informativa e acquisire il consenso:

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO

Informativa e consenso

Come sono informati del trattamento gli interessati? E' stata pubblicata una informativa per pubblici proclami sul sito del promotore

È stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR? SI

È stata pubblicata la valutazione di impatto? sul sito del promotore

Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR

È stata predisposta una procedura ad hoc da parte del Titolare? SI

Come fanno gli interessati a esercitare i loro diritti: Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa.

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO

MISURA	Esistenti	Note
Organigramma interno	X	Ruoli e Responsabilità
Controllo accessi	X	L'accesso avviene tramite account personali. Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore.
Gestione dei cambiamenti	X	Ogni modifica ai sistemi IT è valutata, registrata e monitorata. E' stata definita una procedura generale per la protezione dei dati personali, comprensiva di valutazioni in ottica by design e by default, volta a individuare i requisiti di protezione dei trattamenti e a implementare e mantenere i sistemi e le applicazioni garantendo livelli di sicurezza adeguati. L'acquisizione di componenti del sistema informativo tiene conto dei requisiti di sicurezza dei trattamenti che dovranno essere supportati e delle garanzie offerte dal fornitore.
Strumenti di sicurezza e protezione	X	Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.

Gestione degli incidenti	X	Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log. Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	Il titolare gestisce i rapporti con i propri Responsabili del trattamento attraverso accordi formalizzati che comprendono specifiche clausole per assicurare la riservatezza dei dati trattati e l'obbligo per i Responsabili di operare in conformità alla normativa sul trattamento dei dati personali, in particolare, per quanto riguarda le misure di sicurezza, in riferimento agli art. 28 e 32.
Pseudonimizzazione e cifratura	X	Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati. Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.
Continuità operativa	X	L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km. I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.
Formazione e gestione del personale	X	Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di

		aggiornamento periodici awareness e sensibilizzazione. Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.
Sicurezza delle postazioni di lavoro e delle reti	X	Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware. Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.
Backup e Vulnerability Assessment	X	Backup giornalieri dei dati e test periodici del sistema di ripristino. Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici). I datacenter sono certificati TIER3 e TIER4.

VALUTAZIONE DEL RISCHIO

IMPATTO	PROBABILITA'
MASSIMO	4
IMPORTANTE	3
LIMITATO	2
TRASCURABILE	1

MATRICE DI VALUTAZIONE DEL RISCHIO

Probabilità (P)	Impatto (I)	Rischio (R=P*I)
Probabilità trascurabile: 1 Probabilità limitato: 2 Probabilità importante: 3 Probabilità massima: 4	Impatto trascurabile: 1 Impatto limitato: 2 Impatto importante: 3 Impatto massimo: 4	Rischio basso: R < 6 Rischio medio: 7 < R < 11 Rischio alto: R > 11

Valutazione del Rischio

Accesso Illegittimo ai Dati: Limitato

Modifiche Indesiderate dei Dati: Trascurabile

Perdita di Dati: Trascurabile

Valutazione Complessiva del Rischio: 5

Matrice di Valutazione del Rischio


Description of Image

APPENDICE

MINACCE

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali: Perdita di controllo dei propri dati Utilizzo da parte di terzi di dati dell'interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia: Comportamenti sleali/fraudolenti Attacco informatico (es. social engineering, man in the middle, denial of service, brute force, etc.) Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte: Fonti umane esterne (es. criminali informatici, fornitori, utenti) Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitato

MODIFICHE INDESIDERATE DEI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali: Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia: Errore operativo

Quali sono le fonti di rischio?

Fonte: Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Back – up dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitato

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile

PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali.

Impatti Potenziali

Costi aggiuntivi

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Minaccia: Errore operativo

Quali sono le fonti di rischio?

Fonte: Eventi tecnologici (es. guasti, malfunzionamenti, etc.) Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; Antivirus/firewall; Tracciabilità; Gestione postazioni; Politiche di tutela della privacy; Politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile