



DATA VALIDAZIONE DPIA 03/07/2024

- **Titolo del progetto di ricerca:** LEARNING: neureguLin/hEr pAthway RevisioN In luNG mucinous adenocarcinoma
- **Codice/Acronimo del Protocollo:** LEARNING v1.0
- **Promotore del progetto di ricerca:** Ministero della Salute Italiano
- **Responsabile Scientifico e affiliazione:** Lucia Anna Muscarella, Laboratorio di Oncologia, IRCCS Fondazione Casa Sollievo della Sofferenza
- **Centro Partecipante:** Fondazione IRCCS Casa Sollievo della Sofferenza
- **Sperimentatore Principale presso il Centro Partecipante:** Lucia Anna Muscarella

Nome del DPO/RPD

Mercurio Giuseppe

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Considerata la natura retrospettiva dello studio in oggetto, condotto successivamente all'erogazione della prestazione di cura – considerate le misure di minimizzazione del trattamento dei dati e le modalità di archiviazione degli stessi; considerate le misure di sicurezza dei canali informatici e le politiche di tutela della privacy, nonché la gestione degli incidenti di sicurezza e violazione dei dati personali – il rischio della perdita del controllo dei dati e della violazione della riservatezza residuo risulta limitato. Pertanto il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non è richiesto il consenso degli interessati in quanto lo studio prevede la raccolta dei dati personali in maniera retrospettiva. I dati sono già presenti nei sistemi del titolare del trattamento e raccolti in occasione delle prestazioni sanitarie. A tale riguardo poiché numerosi pazienti sono deceduti o risultati non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003 e nel rispetto di quanto previsto dall'art. 89 GDPR, come documentato nel "MO-PR-8-DichRetro Dichiarazione sostitutiva consenso Retrospettivi_v.2" firmata dal Responsabile Scientifico dello studio, sarà in ogni caso onere della Fondazione cercare di ottenere successivamente il consenso dei pazienti non contattabili qualora questi si presentino presso la Fondazione per ulteriori prestazioni sanitarie o follow-up.

Contesto

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	1 di 19



Panoramica del trattamento

Quale è il trattamento in considerazione?

- La presente valutazione d'impatto prende in considerazione lo studio osservazionale "LEARNING: neureguLin/hEr pAthway RevisioN In luNG mucinous adenocarcinoma"
- L'obiettivo dello studio è quello di condividere nuove conoscenze relative al profilo molecolare dei pazienti con adenocarcinoma invasivo mucinoso del polmone e dei pazienti con carcinoma polmonare non a piccole cellule (NSCLC) sottoposti a trattamento con inibitori delle tirosino chinasi (TKI) tra i Centri coinvolti nello studio. Lo studio, inoltre, consentirà una rapida validazione di un robusto percorso metodologico-diagnostico in grado di rilevare le nuove alterazioni molecolari identificate in campioni biologici di diversa natura. In particolare, ove possibile, verranno studiate le alterazioni nei geni NRG e indagato lo stato di attivazione dei recettori di membrana ErbB utilizzando un ampio ventaglio di metodiche rapide e sensibili di ultima generazione. Il fine ultimo dello studio è quello di identificare nel tessuto e nel sangue dei pazienti oncologici nuove alterazioni molecolari di carattere somatico utili per applicare una medicina personalizzata anche ai pazienti con istologie rare e/o aggressive di carcinoma polmonare. Si chiarisce che questo studio non è una sperimentazione clinica e non prevede la somministrazione di farmaci/trattamenti che esulano dalla normale pratica clinica.

Quali sono le responsabilità connesse al trattamento?

- In relazione al presente studio il Promotore e i Centri Partecipanti agiscono in qualità di autonomi titolari del trattamento, in seguito alle valutazioni fatte congiuntamente in sede di approvazione del protocollo di studio.
- Il PI dello studio è, ai sensi dell'art. 2-quaterdecies del Codice Privacy, autorizzato al trattamento dei dati.

Ci sono standard applicabili al trattamento?

- Prescrizioni e Regole deontologiche, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti (art. 2-quater del Codice e art. 21, comma 5, del d.lgs. 10 agosto 2018, n. 101).
- Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario 7 marzo 2019.
- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21 comma 1 del d.lgs. 10 agosto 2018 n. 101.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	2 di 19



Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati nel contesto della ricerca scientifica sono quelli stabiliti dal protocollo di studi e in particolare:

- dati anagrafici e di contatto (nome, cognome, data e luogo di nascita, luogo di residenza, codice fiscale);
- dati particolari ex art. 9 GDPR (dati relativi alla salute, dati genetici);
- Rif. dati indicati nella lista variabili eCRF

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

- Il personale sanitario impegnato nella ricerca clinica estrae manualmente i dati dalla cartella clinica del paziente e in particolare vengono riportati nella CRF elettronica e in particolare i dati che includono caratteristiche del tumore, dei trattamenti ai quali è stato sottoposto, dei controlli che sono stati effettuati dopo l'intervento chirurgico, nonché i dati relativi ai campioni biologici di pazienti colpiti dalla mutazione oggetto dello studio. Tali dati sono trasferiti in forma pseudonimizzata al Promotore con gli strumenti di condivisione concordati con lo stesso, e sono analizzati per il tempo strettamente necessario alla conduzione dello studio (da un minimo di tre ad un massimo di quattro anni) al termine del quale saranno conservati per un periodo massimo di sette anni ed eventualmente trattati, previa anonimizzazione, per finalità di pubblicazione scientifica e per convegni/seminari.

- Il Promotore non è tenuto a conoscere l'identità dei pazienti, se non in fase di controllo della qualità della ricerca per tramite del monitor e comunque solo on-site per il tempo strettamente necessario ad effettuare tali verifiche.

Quali sono le risorse di supporto ai dati?

- CRF elettronica
- Campioni biologici
- Sistema informativo aziendale
- Postazioni aziendali fisse
- Rete aziendale

Valutazione : Accettabile

Commento di valutazione :

La descrizione dei dati trattati, dei trattamenti previsti nell'intero ciclo funzionale del progetto in valutazione, nonché le risorse a supporto dei dati, permettono di valutare "accettabile" la presente

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	3 di 19



sezione.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

- I dati sono trattati per finalità di ricerca scientifica.

Valutazione : Accettabile

Commento di valutazione :

La descrizione delle finalità del trattamento qui descritta è valutata "accettabile".

Quali sono le basi legali che rendono lecito il trattamento?

- art. 6.1 lett. a) GDPR;

- art. 9.2 lett. a) GDPR.

Valutazione : Accettabile

Commento di valutazione :

La dichiarazione delle basi giuridiche del trattamento è valutata "accettabile".

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

- I dati raccolti seguono un protocollo di ricerca che ne definisce gli obiettivi e il disegno, vengono utilizzati soltanto i dati relativi ai campioni pertinenti con il perimetro dello studio.

- Nel protocollo sono definiti in maniera precisa i criteri di inclusione o esclusione dallo studio, pertanto vengono inclusi soltanto i dati che corrispondono al profilo ricercato.

Valutazione : Accettabile

Commento di valutazione :

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	4 di 19



Le modalità descritte di raccolta dei dati riguardo alla loro adeguatezza, pertinenza e non eccedenza in relazione alle finalità per cui sono trattati sono valutate "accettabili".

I dati sono esatti e aggiornati?

- Per loro natura, per tali progetti nei protocolli non è prevista una fase di riverifica sulla correttezza dei dati che poi vengono analizzati.
- Una ulteriore revisione dei dati di partenza, viene invece effettuata a fronte di successivi progetti di ricerca, pertanto la revisione del dato di partenza (dato clinico) ha effetti solamente su eventuali nuovi studi e non anche su quelli già conclusi.

Valutazione : Accettabile

Commento di valutazione :

La descrizione delle attività svolte dal Titolare per garantire esattezza e aggiornamento dei dati è valutata "accettabile"

Qual è il periodo di conservazione dei dati?

- Lo studio si concluderà il 04/04/2026. A seguito della sua conclusione, i dati saranno conservati per i tempi previsti dalle normative e successivamente distrutti. Non verranno distrutti solo nel caso in cui a) non sia più possibile ricondurli alla sua identità, perché anonimizzati nel corso dello studio stesso; b) in presenza di un suo specifico consenso informato. I dati potrebbero essere trattati poi in forma aggregata e anonima per eventuali pubblicazioni scientifiche o convegni/seminari.

Valutazione : Accettabile

Commento di valutazione

La dichiarazione del periodo di conservazione dei dati è valutato coerente con le specifiche di progetto.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	5 di 19



Gli interessati per cui è applicabile la base giuridica del consenso – art. 6.1 lett. a) e art. 9.2 lett. a) del GDPR – sottoscrivono apposito consenso informato.

Valutazione : Accettabile

Commento di valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Gli interessati per cui è applicabile la base giuridica del consenso – art. 6.1 lett. a) e art. 9.2 lett. a) del GDPR – sottoscrivono apposito consenso informato.

- I dati sono già presenti nei sistemi del titolare del trattamento e raccolti in occasione delle prestazioni sanitarie. A tale riguardo poiché numerosi pazienti sono deceduti o risultati non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003 e nel rispetto di quanto previsto dall'art. 89 GDPR come documentato nell'autodichiarazione formulata dai PI degli studi, sarà in ogni caso onere della PI cercare di ottenere successivamente il consenso dei pazienti non contattabili qualora questi si presentino presso la Fondazione per ulteriori prestazioni sanitarie o follow up.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono esercitare il diritto di accesso:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy della Fondazione, reperibile sia nell'informativa generale che nel sito web istituzionale;
- direttamente presso il P.I. e la sua equipe.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	6 di 19



Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono esercitare il diritto di opposizione e limitazione:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy della Fondazione, reperibile sia nell'informativa generale che nel sito web istituzionale;
- direttamente presso il P.I. e la sua equipe.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare il diritto di opposizione e limitazione:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy della Fondazione, reperibile sia nell'informativa generale che nel sito web istituzionale;
- direttamente presso il P.I. e la sua equipe.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Per questa tipologia di trattamenti, non sono previsti responsabili del trattamento.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

- Per questo studio non è previsto il trasferimento dei dati personali al di fuori dell'Unione Europea.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	7 di 19



Valutazione : Accettabile
Commento di valutazione :
Accettabile

Rischi

Misure esistenti o pianificate

Anonimizzazione

- I dati vengono sottoposti ad anonimizzazione e aggregazione prima della pubblicazione dei risultati della ricerca.

Valutazione : Accettabile
Commento di valutazione :
Accettabile

Controllo degli accessi logici

- Gli accessi in dominio sono concessi dall'UOC Sistemi Informativi, a seguito di richiesta scritta e firmata da parte del Direttore di Unità Operativa.

Valutazione : Accettabile
Commento di valutazione :
Accettabile

Archiviazione

- I dati della ricerca sono caricati su foglio Excel in forma pseudonimizzata, archiviati in file zip, protetti da password forte che viene comunicata separatamente.

Valutazione : Accettabile
Commento di valutazione :
Accettabile

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	8 di 19



Gestione postazioni

- Secondo policy aziendali, i documenti che vengono memorizzati su specifiche aree di share aziendali sono oggetto di backup da parte del personale di ricerca.
- Stessa politica viene adottata per i dati memorizzati su procedure aziendali.
- In ogni caso i dati originali sono sempre disponibili.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Controllo degli accessi fisici

- L'accesso ai locali è bloccato da serrature con codice: il codice di accesso è rilasciato al solo personale che abbia necessità ad accedere a tali locali (anche se condivisi con altri professionisti), oltre al personale del servizio di pulizia.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Sicurezza dell'hardware

- Tutti i dispositivi in dotazione al personale della Fondazione sono equipaggiati con antivirus costantemente aggiornato. Ogni dispositivo in custodia al personale di ricerca può essere utilizzato soltanto da personale formato all'uopo.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Politica di tutela della privacy

- La Fondazione è dotata di un Ufficio Privacy e di un DPO in staff presso l'UO Affari Generali, Legale, Contratti e Tutela della Privacy.

Valutazione : Accettabile

Commento di valutazione :

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	9 di 19



Accettabile

Integrare la protezione della privacy nei progetti

- La Fondazione, conformemente alla disciplina del Reg. (UE) 2016/679, gestisce i dati nel rispetto del principio di privacy-by-design e privacy-by-default.
- I dati trattati sono soltanto quelli strettamente necessari per le finalità perseguite, in ossequio al principio di minimizzazione.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

- La Fondazione gestisce i data breach mediante il coordinamento dell'Ufficio Privacy, d'intesa con le Direzioni aziendali coinvolte.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Gestione del personale

- Il personale della Fondazione, autorizzato al trattamento dei dati, è debitamente formato con cadenza periodica sulla normativa in materia di protezione dei dati personali.
- Il personale viene adeguatamente formato in merito alle attività di trattamento e ai sistemi di sicurezza da adottare.
- Per tale scopo vengono effettuate periodiche sessioni formative con azienda leader del settore della formazione.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Vigilanza sulla protezione dei dati

- La Fondazione ha nominato un responsabile della protezione dati, e rivede con cadenza periodica le procedure e le documentazioni prodotte in ossequio al GDPR.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	10 di 19



Valutazione : Accettabile

Commento di valutazione :

Accettabile

Minimizzazione dei dati

- I dati raccolti seguono un protocollo di ricerca che ne definisce gli obiettivi e il disegno, vengono utilizzati soltanto i dati relativi ai campioni pertinenti con il perimetro dello studio. Nel protocollo sono definiti in maniera precisa i criteri di inclusione o esclusione dallo studio, pertanto vengono inclusi soltanto i dati che corrispondono al profilo ricercato. I dati raccolti saranno trattati esclusivamente per le finalità dello Studio. L'accesso ai dati clinici è consentito solamente al personale sanitario autorizzato, mentre al restante personale (ricercatori), è consentito il trattamento dei soli dati necessari all'attività di ricerca prevista dal singolo progetto.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Lotta contro il malware

- L'intranet aziendale è protetta da sistemi di firewall contro accessi non consentiti.
- Qualora sia richiesta l'abilitazione per un dispositivo personale, questa viene attentamente vagliata, e prima di procedere alla connessione lo stesso dispositivo viene adeguato secondo lo standard di policy aziendale (es. antivirus aziendale).

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Backup

- Secondo policy aziendali, i documenti che vengono memorizzati su specifiche aree di share aziendali sono oggetto di backup da parte del personale di ricerca.
- Stessa politica viene adottata per i dati memorizzati su procedure aziendali.
- In ogni caso i dati originali sono sempre disponibili.

Valutazione : Accettabile

Commento di valutazione :

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	11 di 19



Accettabile

Pseudonimizzazione

- I dati vengono sottoposti ad una procedura di pseudonimizzazione tramite l'assegnazione di un codice identificativo.
- Il promotore non è tenuto a conoscere l'identità dei pazienti reclutati presso ciascun centro partecipante.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Gestione dei terzi che accedono ai dati

- Nell'ambito della ricerca scientifica un terzo autorizzato dal Promotore e potrebbe accedere ai dati in chiaro soltanto recandosi presso il centro partecipante e per il tempo strettamente necessario alla conduzione delle verifiche sulla qualità della ricerca come previsto dal contratto per la sperimentazione, dalle Good Clinical Pratiche e dalla normativa pertinente. In nessun caso il monitor può esportare dati in chiaro o comunicarli direttamente al Promotore, che non ha interesse a conoscere l'identità dei pazienti arruolati, ma soltanto di verificare che i dati acquisiti e studiati dal centro partecipante siano rispettosi del protocollo di studi e della pertinente legislazione.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Crittografia

- Gli archivi che contengono le eCRF sono crittografati.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Rischi

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	12 di 19



Accesso illegittimo ai dati

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

Perdita della riservatezza, Perdita sul controllo dell'utilizzo dei dati, Riutilizzo illecito dei dati personali acquisiti

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Sottrazione delle credenziali di accesso, Attacco al sistema informatico aziendale, Attacco al sistema informatico del promotore, Intercettazione delle comunicazioni

Quali sono le fonti di rischio?

Comportamento improprio personale interno, Comportamento improprio personale esterno, Attaccante esterno

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Gestione postazioni, Backup, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Lotta contro il malware, Pseudonimizzazione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Minimizzazione dei dati

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

Importante, Pur adottando le predette misure di sicurezza e in particolare le misure di minimizzazione, di pseudonimizzazione, sicurezza dell'hardware, sicurezza dei canali informatici e la formazione del personale, la gravità del rischio di perdita del controllo dei dati e della riservatezza residuo risulta comunque elevata in quanto l'eventuale accesso ai dati in chiaro dei pazienti, che sono comunque conservati all'interno della documentazione originale dello Studio, comprometterebbe la loro riservatezza e determinerebbe la mancanza di controllo sull'utilizzo dei dati con degli impatti tanto materiali quanto immateriali significativi vista anche la categoria particolarmente vulnerabile di interessati coinvolti nel trattamento. Si raccomanda pertanto di porre molta attenzione al processo di pseudonimizzazione, alla vigilanza sulla protezione dei dati personali, alla sicurezza dei canali informatici e alla formazione del personale in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale accesso illegittimo.

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

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	13 di 19



Limitata, Date le misure di minimizzazione, di pseudonimizzazione, backup, controllo degli accessi logici, di sicurezza dei canali informatici, cifratura, password forte, archiviazione, formazione del personale, gestione dei terzi che accedono ai dati la probabilità del rischio di eventuale accesso illegittimo dei dati residuale rimane limitata.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Rischi

Modifiche indesiderate dei dati

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

Nessun impatto reale

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

Errata compilazione della CRF

Quali sono le fonti di rischio?

Comportamento improprio personale interno

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

Backup, Pseudonimizzazione

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

Trascurabile, Gli eventuali impatti di una modifica dei dati riguardano i risultati della ricerca e non gli interessati

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

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	14 di 19



Trascurabile, Evento molto improbabile vista l'alta specializzazione e motivazione del personale di ricerca.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Rischi

Perdita di dati

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

Perdita della riservatezza, Perdita sul controllo dell'utilizzo dei dati

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

Perdita delle credenziali d'accesso ai dispositivi aziendali, Sottrazione delle credenziali di accesso, Attacco al sistema informatico aziendale, Attacco al sistema informatico del promotore

Quali sono le fonti di rischio?

Comportamento improprio personale interno, Comportamento improprio personale esterno, Attaccante esterno

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

Controllo degli accessi logici, Backup, Gestione del personale, Minimizzazione dei dati, Vigilanza sulla protezione dei dati, Sicurezza dell'hardware, Controllo degli accessi fisici

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

Importante,

Pur adottando le predette misure di sicurezza e in particolare le misure di minimizzazione e di pseudonimizzazione, il rischio residuo di perdita del controllo dei dati e della riservatezza risulta comunque elevato in quanto l'eventuale perdita dei dati dei pazienti, conservati in chiaro all'interno del sistema informativo della Fondazione in varie forme (appunti, cartella clinica elettronica,

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	15 di 19



documenti clinici archiviati su aree di share aziendale), comprometterebbe la loro riservatezza e la conseguente mancanza di controllo sull'utilizzo dei dati avrebbe degli impatti tanto materiali quanto immateriali data la tipologia di dati trattati e la categoria di interessati coinvolti nel trattamento (pazienti oncologici). Si raccomanda pertanto di porre molta attenzione al processo di pseudonimizzazione, alla vigilanza sulla protezione dei dati personali, alla sicurezza dei canali informatici e alla formazione del personale in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale perdita dei dati oggetto di ricerca.

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

Limitata, Date le misure di minimizzazione, di archiviazione, di sicurezza dei canali informatici, delle politiche di tutela della privacy, delle politiche di gestione degli incidenti di sicurezza e violazione dei dati personali, la probabilità che il rischio si realizzi risulta limitata, pur tuttavia si raccomanda di porre molta attenzione alla formazione e gestione del personale e backup nonché alla corretta implementazione delle politiche della privacy e di minimizzazione in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale perdita di dati.

Valutazione : Accettabile

Commento di valutazione :

Accettabile

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	16 di 19



Rischi

Panoramica dei rischi

Panoramica

Principi fondamentali

Finalità	
Basi legali	
Adeguatezza dei dati	
Esattezza dei dati	
Periodo di conservazione	
Informativa	
Raccolta del consenso	
Diritto di accesso e diritto alla portabilità dei dati	
Diritto di rettifica e diritto di cancellazione	
Diritto di limitazione e diritto di opposizione	
Responsabili del trattamento	
Trasferimenti di dati	

Misure esistenti o pianificate

	Anonimizzazione
	Controllo degli accessi logici
	Archiviazione
	Gestione postazioni
	Controllo degli accessi fisici
	Sicurezza dell'hardware
	Politica di tutela della privacy
	Integrare la protezione della privacy nei progetti
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
	Gestione del personale
	Vigilanza sulla protezione dei dati
	Minimizzazione dei dati
	Lotta contro il malware
	Backup
	Pseudonimizzazione
	Gestione dei terzi che accedono ai dati
	Crittografia

Rischi

	Accesso illegittimo ai dati
	Modifiche indesiderate dei dati
	Perdita di dati

Misure Migliorabili

Misure Accettabili

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	17 di 19



Impatti potenziali

Perdita della riservatezza
Perdita sul controllo dell'...
Riutilizzo illecito dei dat...
Nessun impatto reale

Minaccia

Sottrazione delle credenzia...
Attacco al sistema informat...
Attacco al sistema informat...
Intercettazione delle comun...
Errata compilazione della C...
Perdita delle credenziali d...

Fonti

Comportamento improprio...
Comportamento improprio...
Attaccante esterno

Misure

Controllo degli accessi log...
Gestione postazioni
Backup
Controllo degli accessi fis...
Sicurezza dell'hardware
Gestione del personale
Lotta contro il malware
Pseudonimizzazione
Gestire gli incidenti di si...
Vigilanza sulla protezione...
Minimizzazione dei dati

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Trascurabile

Probabilità : Trascurabile

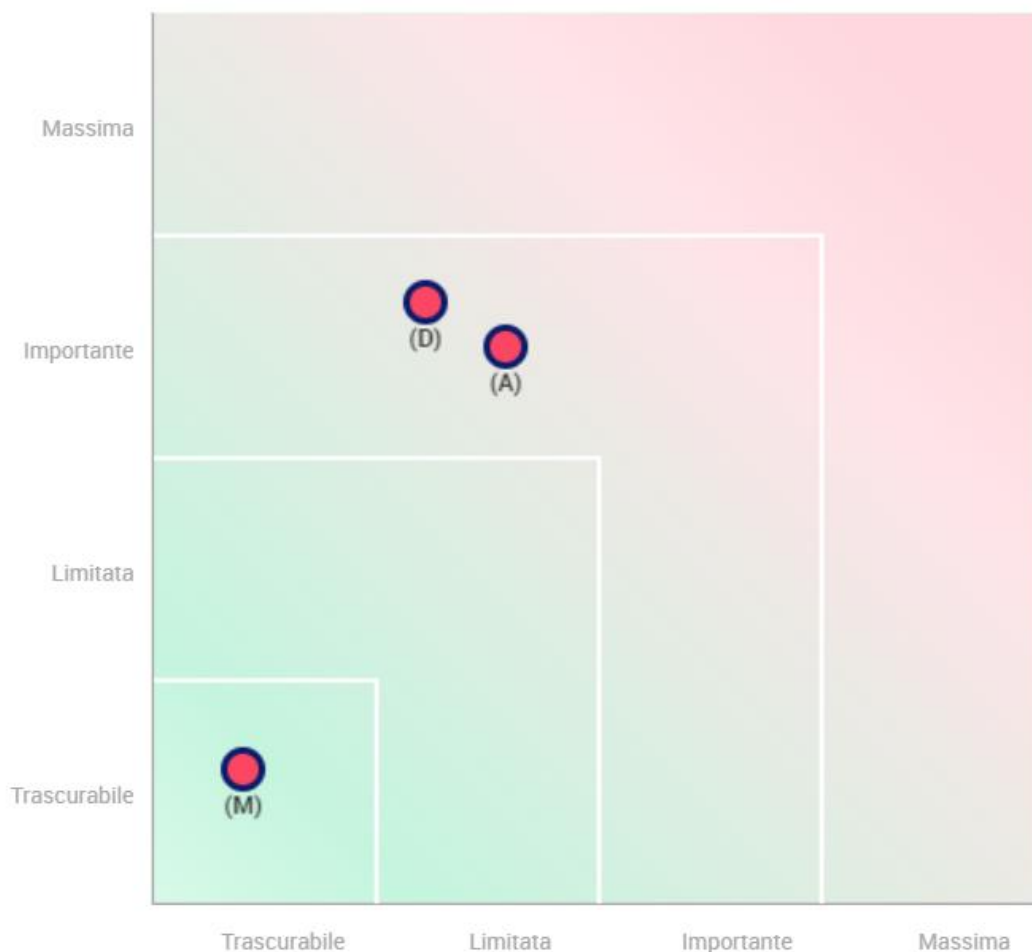
Perdita di dati

Gravità : Importante

Probabilità : Limitata



Gravità del rischio



- **Misure pianificate o esistenti**
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

03/07/24

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-DPIA_RETROSPETTIVI	-	07/06/2024	UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	19 di 19