

**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI  
SVOLTA AI SENSI DELL'ART. 35 DEL REG. UE 2016/679 (G.D.P.R.)**

**Relativa allo Studio**

**no-profit**, nazionale, multicentrico, osservazionale, retrospettivo

*“Niraparib come terapia di mantenimento in pazienti affette da tumore ovarico epiteliale di alto grado, delle tube di falloppio o peritoneale primitivo dopo risposta (parziale o completa) alla chemioterapia di prima linea a base di platino” (MITO 40)“.*

**PROMOTORE**

**Istituto Nazionale Tumori IRCCS “Fondazione G. Pascale” di Napoli**

**INDICE**

1	CONTESTO.....	2
2	PRINCIPI FONDAMENTALI.....	7
3	RISCHI.....	13
4	CONCLUSIONI.....	21

## 1. CONTESTO

### 1.1 Il trattamento in considerazione

Il trattamento dei dati personali oggetto della presente VIP riguarda l'attività dello Studio **no-profit**, osservazionale, multicentrico, nazionale, retrospettivo, di cui l'**Istituto Nazionale Tumori IRCCS "Fondazione G. Pascale" di Napoli** (di seguito denominato anche solo "Fondazione G. Pascale") è Promotore, dal titolo "*Niraparib come terapia di mantenimento in pazienti affette da tumore ovarico epiteliale di alto grado, delle tube di falloppio o peritoneale primitivo dopo risposta (parziale o completa) alla chemioterapia di prima linea a base di platino*" (MITO 40)".

**Lo scopo dello Studio** è registrare tutti i dati relativi alle storie di malattie e, in particolare, quelli relativi alla tossicità (sicurezza) ed efficacia del farmaco Niraparib.

Niraparib è stato sviluppato per ritardare la recidiva del carcinoma ovarico nelle pazienti che hanno completato la chemioterapia.

Questo farmaco orale (sviluppato per ritardare la recidiva del carcinoma ovarico nelle pazienti che hanno completato la chemioterapia) è un potente inibitore di proteine chiamate PARP1 e PARP2 e viene utilizzato nel trattamento di tumori le cui cellule presentano difetti in uno specifico meccanismo di riparazione del DNA, meccanismo chiamato "ricombinazione omologa".

In queste cellule intervengono le proteine PARP che tentano di riparare il DNA danneggiato. Prevenendo questa azione, Niraparib impedisce la riparazione del danno al DNA e quindi la replicazione delle cellule tumorali.

Grazie a questo meccanismo d'azione, Niraparib come terapia di mantenimento ha dimostrato di essere in grado di ritardare la crescita del tumore nelle pazienti affette da tumore ovarico epiteliale di alto grado, delle tube di falloppio e peritoneale primitivo dopo risposta (parziale o completa) alla chemioterapia di prima linea a base di platino indipendentemente dallo stato mutazionale BRCA.

Il trattamento con Niraparib, prescritto dal medico, verrà continuato per un periodo massimo di 36 mesi ma potrebbe essere interrotto a causa di tossicità inaccettabile, progressione della malattia o decisione del medico o del paziente.

L'entrata nello Studio non comporterà un cambiamento della pratica clinica né della strategia di cura elaborata per il paziente al quale non verrà richiesto un impegno aggiuntivo rispetto alle normali visite già previste per la sua malattia.

Lo Studio prevede la raccolta dati relativa a pazienti in trattamento con Niraparib come terapia di mantenimento che hanno risposto alla prima linea di trattamento con platino.

Sarà condotto presso 42 centri clinici italiani, coinvolgerà circa 600 pazienti in totale e verrà svolto sulla base del protocollo di studio e di procedure operative standard identificate dallo Sponsor.

In ragione della natura osservazionale dello Studio, gli Interessati non dovranno sottoporsi né a procedure né a trattamenti farmacologici diversi rispetto a quelli previsti nella normale pratica clinica e, dunque, non vi saranno rischi aggiuntivi rispetto alla pratica clinica.

Tra i pazienti arruolati nello Studio, ne sarà prevista una parte per la quale non sarà possibile raccogliere previamente il consenso al trattamento dei dati poiché, all'esito delle ricerche effettuate, saranno risultati deceduti o non più rintracciabili.

**La Fondazione G. Pascale** ha già sottoposto il Protocollo di studio al Comitato Etico del Centro Coordinatore, dal quale ha ricevuto Parere favorevole alla conduzione dello Studio nonché ai Comitati Etici a cui afferiscono i Centri satellite coinvolti nello Studio, prima della presentazione dell'istanza di consultazione preventiva.

In linea con quanto stabilito nel Protocollo di studio, la **Fondazione G. Pascale** ritiene di procedere:

- a) adottando misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato;
- b) acquisendo il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dal novellato art. 110 del Codice Privacy;
- c) motivando e documentando, anche nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca;
- d) svolgendo e pubblicando la presente valutazione di impatto, ai sensi dell'art. 35 del Regolamento, dandone comunicazione al Garante.
- e) precisando, ai Comitati Etici competenti, che l'ottenimento del consenso informato riguarda tutti i pazienti ancora in vita e contattabili mentre il trattamento dei dati dei pazienti deceduti o non rintracciabili sarà effettuato sulla base del novellato art. 110 del Codice Privacy.

## **1.2 Quali sono le responsabilità connesse al trattamento?**

Il Titolare del trattamento è l'**Istituto Nazionale Tumori IRCCS "Fondazione G. Pascale" di Napoli** con sede legale in Via M. Semmola, Napoli (NA), C. F. e P. I. 00911350635, **in persona del I.r.p.t, Dott. A. M. Bianchi.**

La **"Fondazione G. Pascale"**, quale Titolare del trattamento e Promotore, prima dell'avvio della sperimentazione, ha individuato i Centri partecipanti, predisponendo il protocollo da osservare nel corso dello Studio.

I Centri partecipanti allo Studio non sono assoggettati a vincoli di subordinazione nei confronti del Promotore, disponendo di propria autonomia organizzativa, sebbene nel rispetto del Protocollo, e delle procedure operative del Promotore e gestiscono e custodiscono sotto la propria responsabilità la documentazione di pertinenza.

Pertanto, i singoli Centri di sperimentazione e il Promotore, cui sono imputabili responsabilità distinte nell'ambito dello Studio, si configurano, quali autonomi titolari del trattamento.

Per la realizzazione dello Studio di cui sopra, la **Fondazione G. Pascale** si avvale del supporto di **Clinical Research Technology Srl (di seguito anche solo: "CRT")** con sede legale in Salerno, Via San Leonardo Trav. Migliaro, Salerno (SA) C.F. e P.I.07501100635, che agirà in qualità di CRO (Contract Research Organization), a tale scopo nominata Responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento, dalla **Fondazione G. Pascale.**

### 1.3 Ci sono standard e riferimenti normativi applicabili al trattamento?

#### **Il trattamento oggetto della presente VIP viene effettuato nel rispetto:**

- delle disposizioni del Reg. UE 2016/679 e del Codice Privacy (artt. 5, par. 1, lett. b) e e), 9, par. 2, lett. j) 89 del Regolamento e art. 110 del Codice Privacy);
- delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegato 5 al Provvedimento del 5 giugno 2019;
- delle Regole deontologiche vigenti per trattamenti a fini statistici o di ricerca scientifica allegato A5 al Codice Privacy, 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);
- della nuova formulazione dell'art. 110 del Codice Privacy;
- delle ulteriori garanzie individuate dal Garante nella Deliberazione del 9/05/2024.

Invero, l'art. 44, comma 1-*bis* del decreto-legge 2 marzo 2024, n. 19, convertito con legge 29 aprile 2024, n. 56, recante: *"Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)"* pubblicata nella Gazzetta Ufficiale - Serie Generale n. 100 del 30-04-2024 - Suppl. Ordinario n. 19, ha previsto la modifica della seconda parte dell'art. 110, comma 1 del Codice che oggi dispone che *"Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice"*.

**La presente VIP tiene conto, nelle** more dell'approvazione delle nuove Regole deontologiche, **della nuova formulazione dell'art. 110 del Codice Privacy**, in base alla quale, laddove non sia possibile acquisire il consenso degli interessati e non vi siano altri presupposti normativi, il Titolare del trattamento di dati sulla salute per scopi di ricerca medica, biomedica e epidemiologica non è più tenuto a presentare un'istanza di consultazione preventiva al Garante ma dovrà **rispettare le garanzie individuate da quest'ultimo ai sensi dell'articolo 106, comma 2, lettera d), del Codice** indicate nell'ambito delle Regole deontologiche di cui agli artt. 2-*quater* e 106 del Codice.

Il Garante, in attuazione della disposizione di cui sopra, in data 9 maggio 2024, ha adottato la Deliberazione di promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, prevedendo specifiche garanzie per i titolari del trattamento di dati personali per scopi di ricerca medica, biomedica ed epidemiologica riferiti a soggetti deceduti o non contattabili.

In particolare, in omaggio al principio di *accountability*, il Garante ha previsto che il Titolare motivi in maniera stringente le cause di ordine etico o di impossibilità organizzativa che, negli studi retrospettivi, comportano l'impossibilità di acquisire il consenso.

La presente VIP risulta altresì necessaria ai sensi dell'art. 35 Reg. UE n. 2016/679 (GDPR) e dei Considerando 84, 89, 93, 95 ed alla luce:

- delle Linee Guida WP 248 “in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento UE 2016/679” (in particolare, criteri nn. 3, 4, 5, 7) nonché
- del Provvedimento del Garante per la protezione dei dati personali n. 467 dell’11/10/2018, “Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d’impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, Reg. UE n. 2016/679” (in particolare, criteri n. 3, 6, 10): i titolari del trattamento sono tenuti ad effettuare valutazioni d’impatto sulla protezione dei dati se il trattamento riguarda dati sensibili o aventi carattere strettamente personale o dati riguardanti soggetti interessati vulnerabili.

Nel caso di specie, il trattamento ha ad oggetto dati personali “sensibili” pseudonimizzati relativi a interessati vulnerabili coinvolti in uno Studio clinico multicentrico, su scala nazionale.

Il Titolare, in ogni caso, nel rispetto del principio di accountability, e seguendo la specifica raccomandazione in tema di valutazione d’impatto del WP 29, effettua le VIP anche nei casi in cui non risulti certa l’obbligatorietà delle stesse, ritenendo che la VIP sia “uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati”; (Linee Guida WP 248).

**La redazione del presente documento ha tenuto conto, peraltro, dei provvedimenti e documenti di seguito elencati, ancorché in modo non esaustivo:**

- Con riferimento, in generale, all’applicazione dei principi, delle condizioni di liceità e delle misure di sicurezza relative al trattamento dei dati personali:

*Linee Guida sulla trasparenza ai sensi del regolamento 2016/679 - WP 260; Linee Guida sul consenso ai sensi del regolamento (UE) 2016/679 - WP 259;*

*Linee Guida 4/2019 sull’art. 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita.*

- Con specifico riferimento alla ricerca medica, biomedica ed epidemiologica:

EDPS Parere preliminare sulla protezione dei dati e la ricerca scientifica del 6/01/2020; EDPB Parere 3/2019 sull’interazione tra il regolamento sulle sperimentazioni cliniche ed il Gdpr; Garante Privacy

- Provvedimento n. 146 del 5/06/2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, ex art. 21, comma 1, d.lgs. n. 101/18; Garante Privacy - Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. 9/2016); Garante Privacy – Provvedimento n. 55 del 7/03/2019 in merito all’applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario; Garante Privacy - Linee guida per i trattamenti di dati personali nell’ambito delle sperimentazioni cliniche di medicinali del 24/07/2008; Garante Privacy - Provvedimento n. 515 del 19/12/2018 - Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica; Garante Privacy – Provvedimenti in materia di consultazione preventiva ex artt. 110 Codice Privacy e 36 GDPR: 29/10/2020 n. 202. Doc. web 9517401; 10/12/2020 doc web 9520597; 17/09/2020, doc. web 9479382; 1/11/2021, doc web 9731827; 30/06/2022, doc web 9791886; 6/07/2023, doc. web. 991999.

#### **1.4 Quali sono i dati trattati?**

La realizzazione dell’obiettivo dello studio prevede che i dati raccolti, relativi ai pazienti definiti eleggibili, appartengano alle seguenti macrocategorie:

- dati identificativi

Nello specifico, i dati estratti dalle cartelle cliniche e riportati in CRF per singolo paziente, saranno i seguenti:

Informazioni sociodemografiche: età

Dati relativi alla storia medica: ipertensione pre-esistente, storia di altri tumori, eventuale familiarità Anamnesi oncologica e linee di trattamento, peso, altezza, ECOG all'atto della diagnosi di carcinoma ovarico – età della paziente al momento della diagnosi, istologia del tumore, stadio FIGO, localizzazione del tumore primario, TAC (torace, addome, pelvi).

Trattamento del carcinoma ovarico:

- Orario dell'intervento chirurgico di debulking (primario o di intervallo)
- Esito post chirurgia di debulking (primario o di intervallo): presenza o assenza di malattia residua visibile
- Descrizione delle precedenti linee di chemioterapia (inclusi regimi/farmaci, data di inizio e fine, frequenza)
- Risposta all'ultima linea di chemioterapia/platino
- Settimane trascorse dopo l'ultima somministrazione di platino
- Conta piastrinica all'inizio del trattamento con niraparib
- Qualsiasi anomalia emersa all'analisi dell'emocromo all'inizio e durante il trattamento valutata secondo la standard di cura
- Dose iniziale del trattamento con niraparib
- Intervallo temporale e motivazione dell'eventuale riduzione di dosaggio, con indicazione del nuovo dosaggio assegnata
- Tempistiche e causa dell'eventuale interruzione del trattamento
- Durata del trattamento con niraparib
- Trattamento assegnato in seguito a progressione post niraparib: tipologia ed esito delle successive linee chemioterapiche

Analisi mutazionale (genomica): BRCA/HRD status (biomarcatori analizzati secondo la pratica clinica).

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

Gli obiettivi dello Studio richiedono la raccolta di dati clinici ottenibili dalle cartelle cliniche delle pazienti.

L'attività sarà svolta presso ognuno dei Centri partecipanti, direttamente dallo Sperimentatore Principale e dallo staff da lui specificatamente delegato e consisterà nell'estrazione dei dati inerenti alle pazienti incluse nello Studio dalle rispettive cartelle cliniche

La raccolta dei dati verrà effettuata da personale qualificato evitando condotte che possano determinare indebite pressioni e correggendo tempestivamente eventuali errori ed inesattezze delle informazioni acquisite; i dati saranno utilizzati soltanto dai soggetti autorizzati ed ai soli fini definiti nel progetto di ricerca.

Tali dati saranno inseriti all'interno di un database elettronico attraverso una specifica interfaccia grafica (eCRF), con modalità di Remote Data Entry, da parte dello Sperimentatore Principale e dai membri dello staff opportunamente autorizzati e addestrati allo svolgimento di tale funzione.

Tale database è sviluppato e configurato appositamente per ridurre al minimo l'utilizzazione dei dati personali al di fuori delle finalità dello Studio.

A tutti i pazienti partecipanti allo Studio sarà assegnato un codice numerico personale univoco e progressivo.

Gli sperimentatori prestano la massima attenzione nelle operazioni di data entry nel data base clinico; si precisa che tali operazioni non sono affidate a personale amministrativo.

Il documento contenente le informazioni che permettono la decifratura dei codici sarà detenuto esclusivamente da ciascun Centro di sperimentazione che dovrà custodirlo come documento riservato essenziale alla conduzione dello Studio clinico, in accordo alle indicazioni contenute nella Good Clinical Practice (GCP) ed agli artt. 4, par. 1, n. 5 e 32 Reg. UE 2016/679; ciò al fine di evitare di risalire all'identità dei singoli pazienti coinvolti, fatta eccezione per i soggetti preposti al trattamento dei dati, in qualità di incaricati o responsabili (Sperimentatore Principale e staff da lui delegato, Clinical Monitor).

L'elaborazione dei dati dello Studio memorizzati nel data base è affidata a personale autentificato ed autorizzato in funzione dei ruoli e delle esigenze con credenziali di validità limitata da disattivare al termine dello Studio. L'eCRF sarà accessibile, dai soggetti autorizzati, mediante credenziali di autenticazione personali e non cedibili.

Sono predisposti sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Il database elettronico verrà conservato per il solo tempo necessario a concludere la verifica dei dati e successivamente, terminata l'attività di raccolta ed inserimento e verificatane la completezza ed accuratezza. Dopo la chiusura del database (il database sarà off-line accessibile solo localmente e al solo personale autorizzato alle analisi sui dati attese dal protocollo di studio), tutti i dati raccolti in eCRF saranno conservati dalla **Fondazione G. PASCALE** in un luogo protetto per il tempo necessario al perseguimento degli scopi della raccolta.

Attraverso i protocolli http e SSL, con accesso tramite username e password, sono garantiti elevati livelli di sicurezza e riservatezza delle informazioni, assicurando la trasmissione dei dati tramite un canale di connessione sicuro e cifrato.

Il sistema, inoltre, registra lo storico delle modifiche di ogni dato con indicazione del motivo della modifica e specifica dello username dell'utente che l'ha eseguita.

Il database, configurato appositamente per ridurre al minimo l'utilizzazione dei dati personali al di fuori delle specifiche finalità di ricerca, è installato su server dedicati presso la **Fondazione G. PASCALE** e monitorato direttamente dal personale tecnico del CED aziendale.

Il DB e gli altri file di progetto sono replicati su più server; in ogni server è eseguito backup automatico giornaliero.

Dopo la chiusura del database, si procederà con l'estrazione degli export dei dati pseudonimizzati e all'esecuzione di un'analisi statistica descrittiva che avrà ad oggetto:

- a) verifica obiettivo principale dello studio: osservare l'efficacia di Niraparib come terapia di mantenimento in un contesto di vita reale per le pazienti con carcinoma ovarico di nuova diagnosi;
- b) verifica obiettivo secondario dello Studio: valutare la sicurezza e gli esiti clinici a lungo termine nella stessa popolazione

Ai dati pseudonimizzati contenuti nella eCRF avranno accesso il personale autorizzato del Promotore, dei Centri Clinici, e quello dalla CRO incaricata (Clinical Monitor, Project Manager e Data Manager) nei limiti delle autorizzazioni ricevute.

Lo Sperimentatore Principale e i membri dello staff da lui delegati raccoglieranno i dati personali dalle cartelle cliniche degli Interessati e li inseriranno in forma pseudonimizzata nella e-CRF configurata sulla piattaforma web CRF.NET.

I dati identificativi degli Interessati saranno quindi trattati esclusivamente presso i Centri Clinici da parte dello Sperimentatore Principale e dai membri dello staff da lui delegati, nella fase iniziale di arruolamento e di raccolta retrospettiva dei dati, e durante le attività di monitoraggio da parte dei Clinical Monitor incaricati da CRT.

### **1.6 Quali sono le risorse di supporto ai dati?**

- Piattaforma per il Remote Data Entry di proprietà del Promotore.
- Cartelle dei pazienti in possesso ai Centri partecipanti e presenti su dispositivi informatici e supporti cartacei.
- Server mail per la comunicazione criptata delle informazioni.

## **2. PRINCIPI FONDAMENTALI**

### **2.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?**

**Gli scopi del trattamento dei dati nel contesto dello Studio MITO 40 sono considerati specifici, espliciti e legittimi per diverse ragioni:**

- a) il trattamento dei dati effettuato nell'ambito dello Studio MITO 40 è orientato a raggiungere obiettivi di ricerca chiaramente definiti nel Protocollo e legittimi nel campo della ricerca;
- b) i dati saranno trattati esclusivamente per le finalità dello Studio, per la realizzazione del quale i dati saranno raccolti e inseriti in forma pseudonimizzata nelle eCRF.



## **2.2 Quali sono le basi legali che rendono lecito il trattamento?**

**Le basi giuridiche del trattamento si rinvengono:**

**per i pazienti contattabili**, considerato che il trattamento riguarda anche dati sulla salute per scopi di ricerca medica, nel consenso, ai sensi dell'art. 9, par. 2, lett. a) del Regolamento;

**per i pazienti deceduti o non contattabili**, nella procedura di cui alla nuova formulazione dell'art. 110 del Codice Privacy, unitamente al parere dei comitati etici, oltre che nell'art. 9, par. 2, lett. j) del Regolamento.

**Il consenso** informato degli Interessati alla partecipazione allo Studio e al trattamento dei dati personali verrà raccolto in tutti i casi in cui sarà possibile fornire agli Interessati un'adeguata informazione e quindi acquisirne il citato consenso.

Al fine di assicurare che i soggetti interessati dal trattamento dei dati personali ricevano un'adeguata informazione, è stato predisposto da **Fondazione G. PASCALE**, e fornito ai Centri clinici che partecipano allo Studio, un apposito modello di Foglio informativo e consenso allo Studio e di Informativa e Consenso al trattamento dei dati personali dei pazienti per fini di ricerca.

Il soggetto arruolato riceve, pertanto, due moduli distinti: consenso informato (relativo alla salute) e informativa/consenso (relativo alla privacy).

**La procedura di cui al novellato art. 110 Codice Privacy**, il parere favorevole del competente comitato etico in riferimento all'emendamento allo Studio che prevede il coinvolgimento della corte retrospettiva con particolare riferimento ai pazienti deceduti e/o non rintracciabili e l'adozione di misure idonee alla tutela dei diritti e delle libertà degli Interessati costituiscono la base di liceità del trattamento per i pazienti arruolati che risultino deceduti o non più contattabili.

In ogni caso, i Centri partecipanti daranno inizio ai trattamenti dei dati personali necessari per la realizzazione dello Studio solo dopo lo svolgimento e la pubblicazione della VIP con conseguente comunicazione al Garante di tale adempimento nonché dei definitivi pareri favorevoli dei competenti comitati etici, così integrando la condizione di liceità del trattamento dei dati personali per le finalità perseguite laddove non sia possibile acquisire il consenso degli interessati (Cfr. Provv. n. 202 del 29/10/2020, doc. web 951741; n. 406 del 1/11/2021, doc. web 9731827; n. 73 del 2/03/2023, doc. web 9875254).

## **2.3 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 che verranno trattati sono ottenibili dalle cartelle cliniche dei pazienti.

Sono raccolti e trattati soltanto i dati personali necessari al raggiungimento delle finalità dello Studio.

Tutte le misure, tecniche ed organizzative, sono volte alla minimizzazione dei dati.

## **2.4 I dati sono esatti e aggiornati?**

I dati raccolti nello Studio MITO 40 sono conformi e verificati per garantire la loro accuratezza e aggiornamento.

I Centri coinvolti nello Studio hanno seguito procedure rigorose per la raccolta e verifica dei dati, adottando protocolli standardizzati che includono verifiche da parte di clinical monitor per garantire l'attendibilità e l'accuratezza delle informazioni raccolte.

Sono adottate misure ragionevoli per la rettifica o cancellazione dei dati inesatti.

Il Promotore e gli altri soggetti coinvolti nello Studio prestano particolare attenzione alla formazione del personale, soprattutto con riferimento alle fasi in cui i dati vengono caricati e raccolti dai soggetti di riferimento, ciò al fine di presidiare e mitigare adeguatamente il rischio dell'errore umano; in tal senso, i Centri partecipanti ricevono formazione e specifiche istruzioni scritte.

Si provvede alla registrazione dello storico delle modifiche di ogni dato con indicazione del motivo della modifica e specifica dello username dell'utente che l'ha eseguita.

Per garantire l'effettiva applicazione del principio di esattezza dei dati, in occasione della loro estrapolazione dalle cartelle cliniche dei pazienti, sono predisposte le seguenti misure tecniche ed organizzative:

- gli sperimentatori prestano la massima attenzione nelle operazioni di data entry nel data base clinico e tali operazioni non sono affidate a personale amministrativo;
- i dati non verranno usati senza assicurarsi che essi siano accurati ed aggiornati;
- i dati inesatti rispetto alle finalità del trattamento per le quali sono stati raccolti vengono modificati o rettificati tempestivamente senza ritardi;
- viene eseguito il monitoraggio dei dati raccolti per tutto il ciclo vitale.

Pertanto, le misure, preventive e successive, adottate per limitare il più possibile la possibilità di errore, comprendono: la validazione dei dati, la verifica di coerenza dei dati inseriti; la segnalazione di eventuali errori o problematiche nella raccolta; il rifiuto di raccolta di dati incompleti o imprecisi.

Il monitoraggio delle operazioni di caricamento riguarderà: il momento di caricamento, l'autore ed il tipo di dato inserito.

## **2.5 Qual è il periodo di conservazione dei dati?**

Il periodo necessario per lo svolgimento ed il completamento dello Studio, compreso il trattamento necessario per la finalità di ricerca scientifica, è di tre anni, inteso come il periodo necessario per completare le attività e conseguire le finalità dello Studio (arruolamento e ricerca scientifica); durante questo periodo, verranno condotte tutte le fasi del processo, inclusa la raccolta dei dati e l'analisi e la redazione dei report; la scelta di tale durata massima è basata sulla necessità di garantire un tempo sufficiente per ottenere risultati significativi e condurre un'analisi completa dei dati raccolti; questo periodo tiene conto dei tempi necessari per l'elaborazione dei dati, l'interpretazione dei risultati e la revisione scientifica.

Il periodo di conservazione, presso il Promotore ed i Centri partecipanti, dei documenti essenziali relativi allo Studio (anche per la messa a disposizione dei documenti e dei dati in caso di verifiche o ispezioni delle autorità competenti), verrà individuato in base al principio di accountability.

Tenuto conto di queste ragioni, si ritiene che i dati verranno conservati per un periodo non superiore a quello necessario per conseguire le finalità per le quali sono stati raccolti e trattati e che detto periodo di conservazione sia proporzionato rispetto alle finalità della raccolta.

Il trattamento dei dati da parte della CRO incaricata cessa al termine dello Studio MITO 40, e in seguito, tutti i dati raccolti vanno distrutti in conformità alle disposizioni normative applicabili e alle politiche interne di conservazione e distruzione dei dati.

Al termine del periodo di conservazione i dati verranno anonimizzati/cancellati.

## **2.6 Come sono informati del trattamento gli interessati?**

Verrà raccolto il consenso informato degli Interessati alla partecipazione allo Studio e al trattamento dei dati personali in tutti i casi in cui sarà possibile fornire loro un'adeguata informazione e quindi acquisirne il relativo consenso.

Dunque, i Centri partecipanti effettueranno ogni ragionevole sforzo per contattare tutti i pazienti che soddisfano i criteri di idoneità all'arruolamento nello Studio.

Tuttavia, all'esito di tali attività (che comprendono anche la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente), alcuni dei soggetti interessati potranno risultare deceduti o non rintracciabili al momento dell'arruolamento nello Studio.

Per questi pazienti (i pazienti che dovessero risultare deceduti o non rintracciabili), l'esecuzione dei necessari tentativi per contattarli/rintracciarli sarà documentata dallo Sperimentatore Principale attraverso la compilazione e sottoscrizione di un Modulo di dichiarazione sostitutiva al consenso.

Tali sezioni forniranno dettagli sullo Studio, inclusi i suoi scopi e i criteri di selezione dei partecipanti.

**La Fondazione G. PASCALE** inviterà gli Interessati a mettersi in contatto con le strutture ospedaliere competenti in modo da fornire loro ulteriori informazioni sullo Studio; l'obiettivo di tale modalità di comunicazione è quello di garantire che tutte le persone interessate abbiano accesso alle informazioni pertinenti relative allo Studio MITO 40 ed abbiano la possibilità di prendere una decisione consapevole e informata sulla partecipazione.

Il numero stimato di soggetti interessati che non sarà possibile contattare, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, è stato stimato intorno al 50%.

## **2.7 Come si ottiene il consenso degli interessati?**

**2.7.1** I Centri partecipanti, che hanno il compito di arruolare i pazienti, dovranno preventivamente ottenere da ciascun paziente la sottoscrizione del documento di consenso informato scritto, così come previsto dal Protocollo.

Dunque, gli sperimentatori, per ciascuno dei Centri partecipanti, si impegnano a rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello Studio, sia possibile e, in particolare, laddove questi si rivolgano al Centro, anche per visite di controllo al fine di acquisirne il consenso informato relativo al trattamento dei dati personali.

Per i pazienti deceduti o dispersi non raggiungibili sarà richiesto allo Sperimentatore di documentare in cartella clinica e/o attraverso la compilazione e sottoscrizione di un Modulo di Dichiarazione Sostitutiva al Consenso che l'arruolamento del paziente è avvenuto senza la raccolta del consenso con la relativa motivazione dell'impossibilità della raccolta e l'esecuzione e descrizione dei tentativi fatti per contattare/rintracciare i pazienti.

Verranno, inoltre, adottate idonee forme di pubblicità dell'informativa ; ai sensi dell'art. 14, par. 5, lett. b) del Regolamento, dell'art. 6 delle Regole deontologiche, e della Deliberazione del Garante del 9/05/2024 –mediante diffusione di "Informativa Pubblica" (locandina) presso il Promotore e tutti i Centri partecipanti con lo scopo di raggiungere eventuali pazienti dispersi e non raggiungibili, rimanendo ferma la raccolta del consenso dell'interessato non appena questo dovesse recarsi, per

qualsiasi motivo, al Centro Clinico anche al fine di consentirgli di esercitare i diritti previsti dal Regolamento.

**2.7.2** Si specificano, di seguito, i motivi che giustificano l'impossibilità di riuscire ad informare gli interessati ed acquisirne un valido consenso, nonostante gli sforzi proporzionati e ragionevoli che s'intendono impiegare, secondo quanto previsto dal punto 5.3 delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica e le modalità con le quali verrà accertata l'impossibilità di contattare i pazienti da arruolare:

- i Centri partecipanti effettueranno ogni ragionevole sforzo per contattare tutti i pazienti che soddisfano i criteri di idoneità all'arruolamento nello Studio;
- si stima che, all'esito di tali attività (che comprendono anche la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente), alcuni dei soggetti interessati potranno risultare deceduti o non rintracciabili al momento dell'arruolamento nello Studio;
- l'impossibilità di acquisire il consenso degli interessati verrà attestata solo all'esito di ragionevoli sforzi consistenti in tre tentativi di contatto non andati a buon fine e registrati nella cartella clinica dei pazienti; più precisamente, i soggetti verranno considerati non contattabili dopo tre tentativi telefonici, in tre giorni differenti della settimana e in orari differenti;
- in considerazione del tempo necessario ad effettuare più di tre tentativi telefonici a paziente, un numero superiore di tentativi rappresenterebbe uno sforzo sproporzionato, anche in ragione della natura **no profit** dello studio in oggetto;
- pertanto, su un campione di circa 600 pazienti, dopo aver effettuato tre tentativi di contatto ritenuti proporzionati rispetto all'impiego di risorse economiche per la realizzazione di uno Studio **no-profit** quale quello in esame, alcuni dei soggetti interessati risulteranno deceduti o non rintracciabili al momento dell'arruolamento nello Studio.

Si ritiene di aver comprovato quali siano i ragionevoli sforzi compiuti o che si s'intende compiere all'esito dei quali attestare l'effettiva irreperibilità degli interessati.

**2.7.3** Sussistono, dunque, ragioni particolari ed eccezionali, per le quali contattare i pazienti per acquisirne il consenso è impossibile oppure implica uno sforzo sproporzionato e rischia di pregiudicare il conseguimento delle finalità della ricerca.

La mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che lo Studio intende arruolare nella ricerca, produrrebbe conseguenze significative per lo Studio stesso in termini di qualità dei risultati della ricerca, considerate le seguenti criticità:

- irreperibilità e/o oggettiva impossibilità organizzativa dovuta all'elevata percentuale di pazienti non più seguiti dai Centri partecipanti allo Studio;
- impossibilità organizzativa e/o di fatto dovuta alla lontananza geografica dei pazienti con conseguenti gravi difficoltà e costi del loro ritorno a Centri partecipanti per attuare le procedure di consenso;

- difficoltà nell'utilizzo di strumenti elettronici da parte di pazienti anziani o con scarse competenze ed abilità nel campo elettronico/informatico;
- decessi di pazienti in ragione dell'età avanzata e delle pregresse condizioni cliniche;
- sopravvenuta incapacità di intendere e di volere dovuta all'aggravarsi dello stato clinico.

**2.7.4** Orbene, ove i dati dei pazienti deceduti o non contattabili non fossero inclusi nello Studio, si determinerebbe un pregiudizio alla completezza del campione (e quindi alla accuratezza dei dati) e ciò rischierebbe di pregiudicare gravemente il conseguimento delle finalità dello Studio, in termini di alterazione dei relativi risultati.

Lo Studio, inoltre, non può non ricomprendere anche dati riferiti a soggetti deceduti o non contattabili, pena l'incompletezza e la scarsa rappresentatività del campione.

Infine, limitare la popolazione dello Studio a quei pazienti che si recano di persona ai Centri per le visite di routine durante il periodo di arruolamento previsto ridurrebbe notevolmente e sostanzialmente il numero di pazienti coinvolti nello Studio e ciò renderebbe impossibile o comprometterebbe seriamente il raggiungimento dello scopo della ricerca (una dimensione troppo piccola del campione osservato non sarebbe un'evidenza rappresentativa).

## **2.8 Come fanno gli interessati a esercitare i loro diritti di accesso, portabilità e limitazione dei dati?**

Nel foglio informativo e modello di consenso al trattamento predisposto da **Fondazione G. PASCALE** e fornito ai Centri Clinici è chiaramente indicato che gli Interessati hanno il diritto di esercitare i loro diritti e che per fare ciò possono rivolgersi direttamente al Centro clinico di riferimento.

All'interno del Centro clinico, gli Interessati possono contattare il Referente privacy del trattamento dei dati o la persona autorizzata al trattamento dei dati personali, che operano sotto l'autorità diretta del Titolare. Queste figure sono specificamente designate per gestire le richieste degli Interessati e fornire assistenza per l'esercizio dei loro diritti.

Attraverso questa modalità, gli Interessati hanno la possibilità di richiedere informazioni sui dati personali che sono stati raccolti nel contesto dello Studio MITO 40 e di esercitare i propri diritti se lo desiderano.

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

Qualora siano necessarie modifiche ai dati personali, verranno annotate le modifiche richieste dall'Interessato in appositi spazi.

Questa pratica viene adottata al fine di garantire l'integrità e la tracciabilità dei dati originariamente immessi nell'archivio.

L'annotazione delle modifiche richieste dall'Interessato, senza alterare i dati originariamente immessi nell'archivio, consente di mantenere un registro accurato delle richieste e delle eventuali modifiche apportate, garantendo al contempo la coerenza e l'integrità delle informazioni conservate.

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

Per la realizzazione dello Studio, la **Fondazione G. PASCALE**, in qualità di Titolare del trattamento, si avvale del supporto di responsabili esterni; questi soggetti sono stati selezionati con attenzione e sono tenuti a rispettare rigorosi obblighi di sicurezza e riservatezza dei dati personali.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto regolarmente sottoscritto.

Il contratto sottoscritto con i responsabili del trattamento stabilisce, in modo chiaro, i compiti e le responsabilità di ciascuna parte coinvolta; vengono definiti i limiti e le finalità del trattamento dei dati personali, nonché le misure di sicurezza che devono essere implementate per proteggere tali dati.

Questo contratto fornisce una base legale solida per regolare la relazione tra il Titolare del trattamento e i Responsabili esterni, garantendo che ogni parte sia consapevole dei propri obblighi e delle modalità di trattamento dei dati personali.

In particolare, il Titolare ha sottoscritto con la CRO incaricata, un accordo sulla protezione dei dati personali ai sensi dell'art. 28 Reg. UE 2016/679, nominando CRT Srl Responsabile esterno del trattamento relativo allo Studio.

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

Lo Studio non comporta il trattamento di dati fuori UE. Tuttavia, in caso di eventuale trasferimento dei dati al di fuori dell'Unione Europea, verrebbe garantita una protezione equivalente: il trasferimento sarebbe legittimato da una decisione di adeguatezza ovvero regolato dall'utilizzo di clausole contrattuali standard, conformi alle decisioni dell'Unione Europea in materia di trasferimento di dati personali verso Paesi terzi.

Ciò garantirebbe il rispetto dei diritti degli Interessati ed il trattamento dei dati personali in conformità alle normative vigenti sulla protezione dei dati.

## **3. RISCHI**

### **3.1 Misure di sicurezza esistenti e pianificate**

**3.1.1** L'attività sarà svolta presso ognuno dei 42 Centri partecipanti alla Sperimentazione direttamente dallo Sperimentatore Principale e dallo staff da lui specificatamente delegato e consisterà nell'estrazione dei dati inerenti ai pazienti inclusi nello Studio dalle rispettive cartelle cliniche.

Tali dati saranno inseriti all'interno di un database elettronico attraverso una specifica interfaccia grafica (eCRF), da parte dello Sperimentatore Principale e dai membri dello staff opportunamente autorizzati e addestrati.

Tale database è sviluppato e configurato appositamente per ridurre al minimo l'utilizzazione dei dati personali al di fuori delle finalità dello Studio.

I dati verranno inseriti all'interno della eCRF previa pseudonimizzazione e ogni paziente sarà identificato solo attraverso un codice numerico progressivo.

Dunque, i pazienti sono pseudonimizzati *by design*, mediante assegnazione di un codice paziente univoco. Lo Sperimentatore Principale e i membri dello staff da lui delegati raccoglieranno i dati personali dalle cartelle cliniche degli Interessati e li inseriranno in forma pseudonimizzata nella eCRF. Il documento contenente le informazioni che permettono la decifratura dei codici sarà detenuto esclusivamente da ciascun Centro di sperimentazione che dovrà custodirlo come documento riservato essenziale alla conduzione dello Studio clinico, in accordo alle indicazioni contenute nella Good Clinical Practice (GCP) ed agli artt. 4, par. 1, n. 5 e 32 Reg. UE 2016/679.

Ciò al fine di evitare di risalire all'identità dei singoli pazienti coinvolti, fatta eccezione per i soggetti preposti al trattamento dei dati, in qualità di incaricati o responsabili (Sperimentatore Principale, staff da lui delegato, Clinical Monitor).

L'eCRF sarà accessibile, dai soggetti autorizzati, mediante credenziali di autenticazione personali e non cedibili.

Il database elettronico verrà chiuso al termine dello Studio dopo che ne sarà stata verificata la completezza ed accuratezza.

Attraverso i protocolli http e SSL con accesso tramite username e password sono garantiti elevati livelli di sicurezza e riservatezza delle informazioni, assicurando la trasmissione dei dati tramite un canale di connessione sicuro e cifrato.

I dati identificativi degli Interessati saranno trattati esclusivamente presso i Centri partecipanti da parte dello Sperimentatore Principale e dai membri dello staff da lui delegati, nella fase iniziale di arruolamento e di raccolta retrospettiva dei dati e durante le attività di monitoraggio da parte dei Clinical Monitor incaricati.

### **3.1.2 In merito alla pseudonimizzazione si ribadisce e precisa quanto segue:**

- i dati raccolti ai fini dello Studio saranno trattati con la massima riservatezza e saranno pseudonimizzati con un codice univoco attribuito ai singoli interessati;
- il codice univoco non includerà nessun dato personale direttamente riconducibile al paziente (nome, cognome o numero di cartella clinica o numero di telefono) e sarà utilizzato al posto del nome del paziente e di altre informazioni che direttamente e facilmente lo identifichino;
- il documento contenente le informazioni che permettono di decifrare i codici e risalire all'identità dei pazienti (mediante il collegamento tra i dati personali dei pazienti ed i dati pseudonimizzati) sarà detenuto esclusivamente da ciascun Centro di sperimentazione che dovrà custodirlo come documento riservato essenziale alla conduzione dello Studio clinico, in accordo alle indicazioni contenute nelle Good Clinical Practice (GCP) ed agli artt. 4, par. 1, n. 5 e 32 Reg. UE 2016/679.

**3.1.3 L'anonimizzazione verrà effettuata** attraverso un processo mediante il quale i dati personali verranno modificati in modo irreversibile (al fine di ridurre sensibilmente il rischio di re-identificazione dei pazienti), tenendo conto di quanto previsto nel *Parere 5/2014* del Gruppo di lavoro art. 29.

**Più precisamente, l'anonimizzazione dei dati sarà ottenuta attraverso plurime metodologie finalizzate a minimizzare il rischio di re-identificazione dei soggetti coinvolti nello Studio:**

- eliminazione dalla e-CRF e, conseguentemente, dal database di alcuni parametri;

- generalizzazione mediante aggregazione e K-anonimato (garantendo che ogni valore relativo a un soggetto interessato sia condiviso da almeno un numero minimo (k) di altre persone all'interno dell'insieme, se ciò non avviene verranno aggregati i soggetti in gruppi che contengano almeno k soggetti).

L' "eliminazione" avrà ad oggetto le variabili che conducono alla identificazione diretta degli interessati ("record id" e "patient code") nonché ulteriori variabili ultronee o idonee ad accrescere il rischio di reidentificazione (es. data di nascita, firma del consenso informato).

Infine, verrà rimossa ogni singolarità, qualora, con qualsiasi mezzo, se ne venga a conoscenza in una fase successiva all'applicazione delle tecniche di anonimizzazione e verrà tenuta traccia di tali eventi in modo da ripetere la valutazione del rischio di re-identificazione al raggiungimento del 1% di singolarità individuate sul totale di record inclusi nel dataset (Parere 30/06/2022, doc. web 9791886 e 2/03/2023, doc. web n. 9875254; Provvedimento 31/082023, doc. web n. 9936136).

### **3.2 Accesso illegittimo ai dati**

Se il rischio di accesso illegittimo ai dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli Interessati.

L'accesso illegittimo potrebbe compromettere la privacy dei pazienti interessati, esponendo informazioni personali sensibili a terze parti non autorizzate.

Ciò potrebbe comportare una violazione della riservatezza e dell'autonomia degli Interessati.

I dati personali potrebbero essere utilizzati in modo improprio (ad esempio, per attività di frode o di furto di identità) mettendo gli Interessati a rischio di danni reputazionali; l'utilizzo improprio dei dati potrebbe anche portare a discriminazioni o pregiudizi nei confronti dei pazienti interessati.

L'accesso illegittimo ai dati personali potrebbe compromettere la sicurezza delle informazioni e rendere gli interessati vulnerabili sotto diversi fronti.

Gli Interessati potrebbero perdere il controllo sui propri dati personali e sulla loro diffusione; ciò potrebbe minare la fiducia dei pazienti interessati nel trattamento dei loro dati e nello Studio MITO 40, compromettendo l'efficacia dello Studio.

#### **3.2.1 Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo ai dati includono:

- a) i criminali informatici possono tentare di penetrare nei sistemi informatici al fine di accedere ai dati personali;
- b) i malintenzionati potrebbero cercare di ottenere informazioni sensibili come password o dati personali, inviando comunicazioni fraudolente che sembrano provenire da fonti affidabili;
- c) persone interne all'organizzazione coinvolta nel trattamento dei dati come dipendenti disonesti o negligenti potrebbero abusare o divulgare dati sensibili;
- d) l'eventuale mancanza di adeguate procedure e misure di sicurezza potrebbe facilitare l'accesso illegittimo ai dati;
- e) l'eventuale mancanza di sicurezza fisica potrebbe consentire l'accesso illegittimo ai dati;
- f) le potenziali vulnerabilità dei software utilizzati per il trattamento dei dati possono essere sfruttate da hacker per accedere ai dati personali.



### **3.2.2 Quali sono le fonti di rischio?**

Le fonti di rischio per l'accesso illegittimo ai dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

- a) le vulnerabilità tecniche o di sicurezza presenti nei sistemi informatici coinvolti nelle attività di Studio
- b) la mancanza di adeguate misure di protezione dei dati può facilitare l'accesso illegittimo;
- c) errori commessi da personale interno possono rappresentare una fonte di rischio per l'accesso non autorizzato;
- d) gli attacchi informatici, come il phishing, il malware, i ransomware o gli attacchi DDoS, possono essere posti in essere dagli aggressori sfruttando le vulnerabilità dei sistemi o ingannando gli utenti coinvolti nello Studio;
- e) l'accesso non autorizzato o l'abuso dei privilegi amministrativi o di altro personale autorizzato può compromettere la sicurezza dei dati;
- f) la mancanza di adeguati controlli di accesso e di autenticazione può facilitare l'accesso illegittimo ai dati;
- g) la mancanza di consapevolezza da parte degli utenti sulle pratiche di sicurezza può aumentare il rischio di accesso illegittimo;
- h) il furto o la perdita di dispositivi contenenti dati sensibili possono favorire l'accesso illegittimo ai dati personali.

### **3.2.3 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Per mitigare il rischio di accesso illegittimo ai dati personali, all'interno dello Studio sono state adottate una serie di misure di sicurezza come anche descritte ai punti precedenti:

- a) accesso limitato e controllato ai dati personali del solo personale autorizzato sia a livello fisico che informatico;
- b) pseudonimizzazione dei dati e comunicazione degli stessi tramite chiave crittografica;
- c) protezione fisica dell'infrastruttura informatica utilizzata nello Studio;
- d) monitoraggio e rilevamento delle intrusioni nel sistema da parte dei responsabili esterni fornitori dei software utilizzati per lo Studio;
- e) definizione di politiche e procedure di sicurezza da parte di tutti i soggetti coinvolti nello Studio: Titolare, Responsabili e Cliniche;
- f) formazione del personale coinvolto sui rischi associati all'accesso illegittimo ai dati personali;
- g) audit e controllo delle attività svolte dai responsabili.

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

In ragione della sensibilità dei dati trattati e degli impatti potenziali, l'accesso illegittimo ai dati personali potrebbe causare importanti violazioni della privacy degli Interessati.

Tuttavia, le misure pianificate per mitigare il rischio di accesso illegittimo ai dati e l'adozione di politiche e procedure di sicurezza contribuiscono a ridurre significativamente la gravità del rischio.

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

Le minacce individuate ai punti precedenti devono essere valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando l'elevata frequenza di eventi di data breach nel settore dei dati sanitari, la probabilità del rischio è da considerarsi importante. Tuttavia, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di accesso illegittimo.

### **3.3 Modifiche indesiderate dei dati**

Se il rischio di modifiche indesiderate dei dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli Interessati come di seguito riportati.

Le modifiche indesiderate potrebbero alterare in modo errato o distorto i dati personali, compromettendo la loro accuratezza e affidabilità. Ciò potrebbe influire sulla qualità e sull'affidabilità delle informazioni utilizzate nello Studio MITO 40, portando a conclusioni errate o inesatte.

I Centri partecipanti, il Promotore e soprattutto i pazienti interessati potrebbero perdere fiducia nella correttezza e nell'integrità dei dati personali raccolti e trattati nello Studio e ciò potrebbe influenzare la loro partecipazione allo Studio o la volontà di condividere informazioni sensibili.

Le modifiche indesiderate ai dati personali potrebbero influenzare negativamente le decisioni cliniche prese nell'ambito dello Studio. Se le informazioni modificate vengono utilizzate per formulare diagnosi o piani di trattamento, potrebbe esserci un impatto sulla salute e sulla sicurezza degli Interessati.

Le modifiche indesiderate dei dati potrebbero portare a discriminazioni o pregiudizi nei confronti degli Interessati. Ad esempio, se le informazioni sono alterate in modo da creare false rappresentazioni di una condizione medica o di un rischio associato, gli Interessati potrebbero subire conseguenze negative.

Le modifiche indesiderate dei dati potrebbero avere conseguenze legali per lo Studio MITO 40. Potrebbero essere necessarie azioni legali per correggere gli errori o le distorsioni dei dati, oltre a possibili richieste di risarcimento danni o azioni legali avanzate da parte degli Interessati a seguito di tali modifiche indesiderate.

#### **3.3.1 Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Le principali minacce che potrebbero concretizzare il rischio di modifiche indesiderate dei dati includono:

- a) criminali informatici possono tentare di penetrare nei sistemi informatici al fine di modificare i dati personali;
- b) persone interne all'organizzazione coinvolta nel trattamento dei dati, come dipendenti o amministratori di sistema, potrebbero abusare dei propri privilegi di accesso per apportare modifiche non autorizzate ai dati personali;
- c) errori umani, come la manipolazione erronea dei dati o l'inserimento di informazioni errate, potrebbero portare a modifiche indesiderate dei dati;

- d) l'infezione da malware, come virus, worm o ransomware, potrebbe compromettere la sicurezza dei sistemi informatici e consentire agli aggressori di apportare modifiche indesiderate ai dati personali;
- e) durante il trasferimento dei dati da un sistema all'altro, potrebbero verificarsi vulnerabilità che consentono la manipolazione non autorizzata dei dati.

### **3.3.2 Quali sono le fonti di rischio?**

Le fonti di rischio per le modifiche indesiderate dei dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

- a) gli errori commessi dagli operatori durante l'inserimento, la manipolazione o la gestione dei dati;
- b) l'accesso non autorizzato da parte di individui o entità esterne;
- c) le persone interne all'organizzazione coinvolta nel trattamento dei dati potrebbero abusare dei propri privilegi di accesso per apportare modifiche indesiderate;
- d) gli attacchi informatici, come malware, virus o ransomware, potrebbero compromettere la sicurezza dei sistemi informatici e consentire a terze parti di apportare modifiche indesiderate ai dati;
- e) durante il trasferimento dei dati da un sistema all'altro su reti non sicure o durante l'elaborazione dei dati da parte di terze parti coinvolte nel trasferimento, potrebbero verificarsi vulnerabilità;
- f) la mancanza di adeguate misure di sicurezza può rendere i dati vulnerabili alle modifiche indesiderate.

### **3.3.3 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Per mitigare il rischio di modifiche indesiderate dei dati, all'interno dello Studio sono state adottate una serie di misure di sicurezza come anche descritte ai punti precedenti:

- a) implementare un sistema di gestione degli accessi che permetta solo alle persone autorizzate di accedere ai dati e limitare i privilegi di accesso in base al ruolo e alle responsabilità dell'utente;
- b) utilizzare strumenti di monitoraggio e rilevamento delle attività anomale da parte dei software provider per identificare potenziali tentativi di modifiche indesiderate o accessi non autorizzati;
- c) implementare procedure per la gestione delle modifiche ai dati, compresa l'autorizzazione delle modifiche e la verifica dell'integrità dei dati tramite la figura del clinical monitor;
- d) effettuare regolari backup dei dati che consentano il ripristino in caso di manomissione;
- e) implementare sistemi di autenticazione per garantire che solo le persone autorizzate possano accedere ai dati;
- f) utilizzare la pseudonimizzazione e la criptazione delle comunicazioni in modo che anche se i dati vengono compromessi, non possono essere letti o utilizzati da persone non autorizzate;
- g) fornire formazione sulla sicurezza dei dati a tutti i dipendenti coinvolti nel trattamento dei dati;

- h) implementare politiche e procedure di sicurezza che stabiliscano le responsabilità, i ruoli e le azioni da intraprendere per garantire la protezione dei dati;
- i) effettuare regolare monitoraggio delle attività dei soggetti coinvolti come responsabili.

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

La sensibilità dei dati trattati e il potenziale impatto sulle persone interessate rendono la gravità del rischio di modifiche indesiderate e non autorizzate dei dati personali considerabile come importante in quanto potrebbe compromettere l'integrità delle informazioni degli interessati con gravi conseguenze come evidenziato ai punti precedenti.

Tuttavia, sono state implementate misure specifiche per contribuire a ridurre la gravità del rischio di modifiche indesiderate dei dati e i potenziali impatti negativi sugli Interessati.

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

Le minacce individuate ai punti precedenti devono essere valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando l'elevata probabilità di errori umani, di negligenza del personale o di attacchi informatici nel settore dei dati sanitari, la probabilità del rischio è da considerarsi importante. Tuttavia, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di modifiche indesiderate dei dati.

## **3.4 Perdita di dati**

Vista la natura osservazionale dello studio MITO40 tutti i dati che verranno raccolti saranno una copia dei dati già presenti nelle cartelle cliniche custodite presso i centri che partecipano allo studio. Pertanto una eventuale perdita dei dati verrebbe gestita attraverso una nuova registrazione degli stessi dati prelevandoli dalle cartelle cliniche presenti presso i centri.

### **3.4.1 Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Le principali minacce che potrebbero concretizzare il rischio di perdita di dati sono:

- a) eventi come incendi, allagamenti, danni fisici ai dispositivi di archiviazione o guasti tecnici;
- b) gli errori umani, come la cancellazione accidentale di dati, la sovrascrittura di file importanti o l'errata configurazione dei sistemi;
- c) gli hacker o i criminali informatici possono mirare ai sistemi informatici per distruggere i dati;
- d) la perdita o il furto di dispositivi di archiviazione può mettere a rischio la sicurezza dei dati;
- e) le vulnerabilità dei sistemi, le violazioni delle politiche di sicurezza o l'accesso non autorizzato ai dati da parte di personale interno possono costituire una minaccia per la sicurezza dei dati e causare la loro perdita.

### **3.4.2 Quali sono le fonti di rischio?**

Le fonti di rischio per la perdita dei dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

- a) le infrastrutture tecnologiche che ospitano e gestiscono i dati in quanto possono essere soggette a guasti, errori di configurazione o vulnerabilità di sicurezza che possono portare alla perdita dei dati;
- b) i processi operativi all'interno di un'organizzazione possono essere vulnerabili a errori umani, negligenze o mancanze di procedure adeguate, aumentando il rischio di perdita di dati;
- c) le minacce informatiche possono violare la sicurezza dei sistemi informatici e condurre alla perdita di dati;
- d) le azioni o le negligenze umane possono essere una fonte significativa di rischio per la perdita dei dati;
- e) eventi naturali, come incendi, allagamenti, terremoti o furti, possono danneggiare l'infrastruttura fisica in cui i dati sono conservati, portando alla loro perdita;
- f) la dipendenza da fornitori di servizi esterni per l'archiviazione, la gestione o il trattamento dei dati può comportare rischi, come la perdita dei dati a causa di violazioni della sicurezza o di errori da parte dei fornitori.

### **3.4.3 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Per mitigare il rischio di perdite indesiderate dei dati, all'interno dello Studio sono state adottate una serie di misure di sicurezza come anche descritte ai punti precedenti:

- a) eseguire regolarmente backup e archiviazione dei dati utilizzando i software debitamente forniti per lo Studio;
- b) utilizzare la crittografia per proteggere i dati in transito;
- c) implementare controlli di accesso e autenticazione per limitare l'accesso ai dati solo al personale autorizzato;
- d) i responsabili esterni che utilizzano i software monitorano e rilevano le anomalie per identificare comportamenti sospetti o attività non autorizzate;
- e) fornire una formazione adeguata al personale per sensibilizzarli sulla sicurezza dei dati;
- f) eseguire regolarmente audit sui responsabili esterni che trattano i dati;
- g) stipulare contratti e accordi con fornitori esterni che gestiscono o trattano i dati.

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

La sensibilità dei dati trattati e il potenziale impatto sulle persone interessate rendono la gravità del rischio di perdita dei dati personali considerabile come importante in quanto potrebbe compromettere la validità dell'intero Studio oltre ad arrecare gravi danni agli Interessati stessi che si vedrebbero privati di dati importanti relativi al proprio stato di salute come evidenziato ai punti precedenti.

Tuttavia, sono state implementate misure specifiche per contribuire a ridurre la gravità del rischio di perdita dei dati e i potenziali impatti negativi sugli Interessati.

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

Le minacce individuate ai punti precedenti devono essere valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando

l'elevata probabilità di errori umani, di negligenza del personale, di attacchi informatici nel settore dei dati sanitari o di eventi naturali, la probabilità del rischio è da considerarsi importante. Tuttavia, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di modifiche indesiderate dei dati.

#### **4. CONCLUSIONI**

La valutazione d'impatto effettuata, considerata l'analisi dei rischi, eseguita sotto il profilo della gravità e della probabilità del verificarsi di minacce rilevanti sotto il profilo della protezione dei dati personali, consente di ritenere che l'adozione delle misure tecniche ed organizzative individuate determini la mitigazione dei rischi entro limiti accettabili e di confermare la necessità e proporzionalità del trattamento.

Napoli,

Il Richiedente  
Istituto Nazionale per lo Studio e la Cura  
dei Tumori – IRCCS Fondazione G. Pascale

in persona del suo l.r.p.t.  
dott. Attilio A. M. Bianchi

---