VALUTAZIONE D'IMPATTO, SVOLTA AI SENSI DELL'ART. 35 DEL REGOLAMENTO

1. CONTESTO

1.1 Quale è il trattamento in considerazione?

Il trattamento dei dati personali oggetto della presente DPIA riguarda l'attività dello studio osservazionale retrospettivo prospettico multicentrico di cui il GOIRC è Promotore, dal titolo "Analisi retrospettiva di pazienti con carcinoma a cellule renali metastatico trattati con CABOzantinib: una firma GENomica per descrivere la risposta di lunga durata (CABOGEN)".
Lo studio è finalizzato al miglioramento della pratica clinica quale parte integrante dell'assistenza sanitaria e non a fini industriali, coerentemente con quanto previsto nel Decreto del 30 novembre 2021 "Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione dei dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c) del D-lgs 14 maggio 2019 n. 52".
Lo Studio non rientra nell'ambito di applicazione del Regolamento 536/2014 sulla sperimentazione clinica dei medicinali per uso umano.
Lo studio sarà condotto presso 12centri clinici italiani, coinvolgerà circa 80 pazienti in totale e verrà svolto sulla base del protocollo di studio e di procedure operative standard identificate dallo Sponsor.
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.
Il GOIRC ha sottoposto il Protocollo di studio ai Comitati Etici territorialmente competenti, dei dodici centri clinici coinvolti nello studio, prima della presentazione della suddetta istanza.
In linea con quanto stabilito nel Protocollo di studio alla sezione 10.2, con quanto richiesto nel parere favorevole emesso dal Comitato Etico (CE) del centro coordinatore CEAVEN (segreteria di Reggio Emilia) e con quanto richiesto nel parere favorevole condizionato emesso dal CE del centro satellite CEAVEN (segreteria di Modena), il GOIRC ha successivamente ritenuto di procedere:

a) con la consultazione preventiva al Garante in quanto elemento della condizione di liceità del trattamento dei dati personali per le finalità dello Studio, laddove non sia possibile acquisire il consenso degli interessati;
b) con la notifica, a tutti i Comitati Etici già interpellati, che l'avvio dello studio, e dunque l'inizio del trattamento dei dati personali, sarà subordinato non solo all'ottenimento di parere favorevole rilasciato dagli stessi, ma anche all'ottenimento di provvedimento favorevole da parte dell'Autorità preposta;
c) con la precisazione, a tutti i Comitati Etici già interpellati, che il criterio di inclusione citato alla sezione 4.1 del Protocollo di studio "il consenso informato firmato deve essere ottenuto per tutti i pazienti ancora in vita. I pazienti deceduti o non rintracciabili saranno analizzati in base all'autorizzazione n. 9/2016 del Garante italiano della Privacy" va inteso nel senso che tali pazienti saranno analizzati sulla base del combinato disposto del Provvedimento 146 del 5 giugno 2019 - Allegato 5 Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016) e dell'art. 110, comma 1, ultimo capoverso del Codice come peraltro stabilito alla sezione 10.2 del Protocollo di studio;
d) con la modifica del modulo di Foglio Informativo e Consenso allo studio in cui viene prevista la possibilità per il paziente di scegliere se essere informato o meno o, se rendere disponibili ai familiari, informazioni in merito ai risultati delle indagini genetiche in presenza di incidental findings.

1.2 Quali sono le responsabilità connesse al trattamento?

Il Gruppo Oncologico Italiano di Ricerca Clinica (di seguito GOIRC), con sede legale in Viale Antonio Gramsci, 14, 43100 Parma (PR), C. F. 92009810349, P. I. 02069280341, in persona del presidente del Consiglio Direttivo Prof. Antonino Musolino è il Titolare del trattamento.

GOIRC, quale Promotore, prima dell'avvio della sperimentazione, ha individuato i Centri partecipanti, predisponendo il protocollo da osservare nel corso dello studio, non effettua attività di raccolta diretta dei dati, né ha avuto o avrà contatto diretto con i soggetti inclusi nella sperimentazione; ciò compete ai medici sperimentatori.

I centri partecipanti allo studio non sono assoggettati a vincoli di subordinazione nei confronti del promotore GOIRC, 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 degli studi clinici, si configurano, quali autonomi titolari del trattamento.

Per la realizzazione dello Studio di cui sopra, il GOIRC si avvale del supporto dei seguenti soggetti:

a) Ecol Studio S.p.a., con sede legale in Via Lanzone, 31 20123 Milano (MI), C.F. 01484940463, P.I. 14996171006 che agirà in qualità CRO (Contract Research Organization), a tale scopo nominata responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento da GOIRC.
    a. Nubilaria S.r.l., con sede legale in Baluardo La Marmora,13, 28100 Novara (NO), P.I. 01943340032, che agirà in qualità di sviluppatrice e-CRF, nel quale vengono raccolti i dati di ogni paziente arruolato negli studi clinici gestiti da Ecol Studio S.p.a., a tale scopo nominata quale sub-responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento da Ecol Studio S.p.a.;
b) Roche S.p.a. con sede legale in Viale G. B. Stucchi, 110, 20900 - Monza (MB), P.I. 00747170157, che agirà in qualità di laboratorio per la profilazione genomica tumorale attraverso l'analisi di campioni di tessuto paraffinato o sezioni di tessuto e campioni di sangue intero circolante, a tale scopo nominata responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento da GOIRC;
    a. FMI Germany GmbH, con sede legale in Nonnenwald 2/Building 433, 82377 Penzberg, Germania, che agirà in qualità di laboratorio di analisi per Roche S.p.a, a tale scopo nominata sub-responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento da Roche S.p.a.
    b. Foundation Medicine Inc. con sede legale in 150 Second Street, Cambridge, 02141, MA, USA, che svolgerà le attività necessarie all'analisi dei dati genomici acquisiti, a tale scopo nominata sub-responsabile esterno del trattamento, ai sensi dell'art. 28 del Regolamento da Roche S.p.a.

1.3 Ci sono standard applicabili al trattamento?

a) Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica adottate dal Garante, ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, con provvedimento n. 515, del 19 dicembre 2018. Queste regole deontologiche forniscono linee guida importanti per garantire che il trattamento dei dati personali a fini statistici o di ricerca scientifica avvenga nel rispetto delle leggi sulla privacy.
b) Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegato n. 5 al Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice, del 5 giugno 2019. Queste prescrizioni forniscono ulteriori dettagli e regole specifiche per il

trattamento dei dati personali a fini di ricerca scientifica, assicurando la conformità con le leggi sulla protezione dei dati.

c) Inoltre, Ecol Studio è certificata ISO 9001:2015, il che significa che l'organizzazione ha implementato un sistema di gestione della qualità conforme agli standard internazionali.

La divisione Yghea di Ecol Studio è autocertificata e conforme al DM 15/11/2011, che stabilisce i requisiti minimi per le organizzazioni di ricerca a contratto (CRO). Questo dimostra l'adesione a standard e requisiti specifici per garantire la qualità e la conformità nei processi di ricerca e trattamento dei dati.

1.4. Quali sono i riferimenti normativi applicabili al trattamento?

La presente VIP (Valutazione d'Impatto sulla protezione dei dati) si rende necessaria ai sensi degli artt. 110 D.lgs. 196/03, come riformato dal d.lgs. 101/18 e 36 Reg. UE n. 2016/679 (GDPR).

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 nn. 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.

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 DPIA 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, in particolare, dei provvedimenti e documenti di seguito elencati, ancorché in modo non esaustivo: 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.

1.5Quali sono i dati trattati?

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

- codice di identificazione del paziente;
- dati sociodemografici;
- storia medica incluso lo stadio tumorale;
- diagnosi e trattamenti medici effettuati;
- dati inerenti alle linee di terapie eseguite;
- dati su eventuali reazioni avverse al trattamento con Cabozantinib;
- dati inerenti all'analisi del profilo genomico.

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

Informazioni sociodemografiche:

- età alla diagnosi
- sesso
- razza
- ECOG Performance Status (stato di validità) alla diagnosi

Dati relativi alla storia medica:

- presenza di anamnesi medica significativa fino all'inizio di Cabozantinib
- presenza di patologia/malattia/chirurgia in corso

Anamnesi oncologica e linee di trattamento:

- data della diagnosi
- presenza di biopsia e relativa data
- presenza di nefrectomia e relativa data
- presenza di necrosi tumorale
- presenza di componente sarcomatoide
- stadio della malattia alla diagnosi
- classificazione tumorale - TNM
- gruppo di rischio IMDC (International Metastatic Renal-Cell Carcinoma Database Consortium's)
- data della malattia metastatica
- numero e siti di metastasi all'inizio del Cabozantinib
- presenza di terapia adiuvante, farmaco utilizzato, numero dei cicli, data di inizio e fine, miglior risposta
- presenza di linee di terapia, farmaco utilizzato, numero dei cicli, data di inizio e fine, miglior risposta
- presenza di linea di terapia con Cabozantinib, peso all'inizio del trattamento, ECOG Performance Status all'inizio del trattamento, età all'inizio del trattamento, data di inizio e fine trattamento, dosaggio all'inizio del trattamento, presenza di riduzioni di dosaggio durante il trattamento e relative dosi e date, miglior risposta e relativa data, presenza di progressione di malattia e relativa data, dati relativi alla continuazione/discontinuazione del trattamento e, in quest'ultimo caso, relative ragioni

Sicurezza di Cabozantinib:

- presenza di eventi avversi correlati al trattamento con Cabozantinib, verbatim, grado, data di inizio e fine

Analisi mutazionale (genomica):

- anno di prelievo del campione tumorale del paziente
- origine del campione tumorale raccolto
- sito di provenienza del campione tumorale metastatico
- identificativo del campione tumorale (corrispondente all'ID attribuito al paziente)
- utilizzabilità del campione per lo studio
- data di analisi/rapporto del campione
- presenza di mutazioni e, in caso positivo, descrizione delle stesse tratte dal rapporto

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

Lo scopo di questo studio è descrivere il profilo genomico, ovvero i geni e le mutazioni, di pazienti con carcinoma renale metastatico (mRCC) che rispondono a lungo termine al trattamento con cabozantinib e di pazienti che non rispondono a lungo termine al trattamento con cabozantinib.

Il trattamento medico del carcinoma renale metastatico (mRCC) è cambiato significativamente negli ultimi anni, ma ad oggi non ci sono dati sul meccanismo per definire una popolazione di pazienti che può sperimentare una risposta di lunga durata a cabozantinib nelle seconde linee di terapia, terze o successive.
Obiettivi secondari sono la descrizione di OS (overall survival), ORR (objectiveresponse rate) e DOR (duration of response) in base al profilo genomico rilevato, e la descrizione del profilo genomico in base alla linea di trattamento (seconda, terza o successiva) e alle caratteristiche anamnestiche (peso, ECOG PS, sedi di metastasi, risposta a precedenti linee di trattamento).
Gli obiettivi sopra esposti richiedono la raccolta di dati clinici ottenibili dalle cartelle cliniche e l'utilizzo di campioni di tessuto da nefrectomia o da un sito metastatico per eseguire il profilo genomico con un saggio di sequenziamento di nuova generazione "FoundationOne®CDx (F1CDx)" basato sulla cattura ibrida che permette di studiare le caratteristiche del DNA del tumore, in particolare analizzando 324 geni noti per essere associati al cancro.
L'analisi verrà eseguita in un singolo laboratorio certificato "Foundation Medicine", con sede a Penzberg in Germania.
Il campione di tessuto oggetto di analisi proviene dal blocchetto del campione tumorale del paziente, conservato in paraffina, che è stato prelevato al momento della diagnosi iniziale della malattia (tumore primitivo o metastasi). Il campione di tessuto è attualmente conservato presso l'anatomia patologica di ciascun centro clinico.
Al termine delle analisi il campione sarà restituito al centro clinico di provenienza.
L'attività sarà svolta presso ognuno dei 12 centri, 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 e dai referti del test di profilazione genomica, eseguiti da Roche S.p.a. tramite lo strumento "FoundationOne®CDx (F1CDx)" sui campioni di tessuto dei pazienti.
La raccolta dei dati viene 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 (eCRF), con modalità di Remote Data Entry, 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 del presente studio. I dati verranno inseriti all'interno della CRF previa pseudonimizzazione e ogni paziente sarà identificato solo attraverso un codice numerico.
Gli sperimentatori prestano la massima attenzione nelle operazioni data entry nel data base clinico e 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 (Sperimentatori, Ricercatori, Clinical Monitor).
L'elaborazione dei dati dello studio memorizzati nel data base è affidata a personale autenticato 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.
Non sono previsti dati provenienti da fonti esterne (es. risultati di analisi di laboratorio centralizzato) da immettere in eCRF in modo automatico.
Sono predisposti sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie. Il database elettronico verrà chiuso al termine dello studio dopo che ne sarà stata verificata la completezza ed accuratezza.

Dopo la chiusura del database e poco prima della rimozione dello stesso, tutti i dati raccolti in eCRF saranno consegnati al GOIRC su idoneo supporto magnetico oppure trasferiti mediante piattaforma di condivisione file tramite web o altre modalità, con le opportune protezioni e saranno conservati dal GOIRC in un luogo protetto per il tempo necessario al perseguimento degli scopi della raccolta al termine del quale saranno distrutti.
Prima della consegna, i file saranno compressi e protetti da password e la password sarà comunicata al GOIRC a parte, in forma scritta. Il ricevimento e la corretta leggibilità dei file saranno documentati.
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 è installato su server dedicati presso la server farm Aruba S.p.a., dotata di sistema per la gestione qualità certificato ISO 9001:2015, di sistema per la gestione della sicurezza delle informazioni certificato ISO 27001:2013 e di sistema per la gestione dei data center certificato ANSI/TIA-942-A.
Il DB e gli altri file di progetto sono replicati in più server ospitati in siti diversi in Italia; in ogni server è eseguito backup automatico giornaliero.
Dopo la chiusura del database, si procederà con l'estrazione degli export dei dati pseudonimizzati e il loro trasferimento al GOIRC che procederà all'esecuzione di un'analisi statistica di tipo descrittivo che avrà ad oggetto:

a. il profilo genomico dei pazienti e le caratteristiche basali come peso, ECOG PS, classificazione del punteggio IMDC, siti di metastasi, risposta a precedenti trattamenti in base al profilo genomico dei pazienti.
b. la sopravvivenza globale calcolata dalla data di inizio del trattamento fino alla data di morte per qualsiasi causa o data dell'ultimo contatto in caso di censura.
c. durata della risposta calcolata come il tempo dalla documentazione della risposta del tumore alla progressione della malattia.
d. risposta complessiva: considerata come la percentuale dei pazienti con Complete Response (CR) e Partial Response (PF).

Con riferimento al trattamento dei dati genetici, la trasmissione degli stessi qualora eventualmente dovesse avvenire a mezzo posta elettronica, avverrà in forma di allegato e non come testo. Sarà prevista la cifratura dei dati rendendo nota al destinatario la chiave tramite canale separato, l'allegato sarà protetto con password resa nota separatamente.
Verrà garantito il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente gli interessati. Saranno presenti sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti designati e dei dispositivi in loro possesso. L'accesso ai locali contenenti i dati genetici sarà possibile solo previa identificazione delle persone autorizzate che accedono eventualmente dopo l'orario di chiusura.
Ai dati pseudonimizzati contenuti nella eCRF avranno accesso il personale autorizzato del GOIRC, dei Centri Clinici, e quello dalla CRO Yghea (Clinical Monitor, Project Manager e Data Manager) nei limiti delle autorizzazioni ricevute.
Per lo svolgimento delle attività legate allo sviluppo e al mantenimento della eCRF, la CRO si avvarrà di una terza parte, la società NubilariaSrl con sede legale in Italia, nominata sub responsabile del trattamento.
La Società NubilariaSrl svolgerà in particolare attività di noleggio e manutenzione della piattaforma ACTIDE, hosting dei dati in server dedicati e noleggio di linee certificate di trasmissione dei dati. L'attività svolta è dunque di natura meramente tecnica, Nubilaria non ha alcun ruolo attivo nella raccolta dei dati che saranno quindi trattati come di seguito indicato.
I pazienti sono pseudonimizzati by design, ACTide assegna un codice paziente univoco e Nubilaria non è in possesso di documentazione con dati identificativi dei pazienti.

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 ACTIDE. 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 dalla CRO Yghea. Fuori da tali ipotesi, i dati saranno trattati solo in forma pseudonimizzata o aggregata e non saranno diffusi a soggetti diversi dal GOIRC, dai Centri e dalla CRO per le finalità della conduzione dello Studio.

1.7 Quali sono le risorse di supporto ai dati?

Software Nubilaria: Nubilaria è certificata in accordo a ISO 9001:2015 e ISO 27001:2013 ed il campo di applicazione sono tutti i servizi offerti, inclusi: ACTIDE e-CRF, nella versione 2.3.9 e ACTIDE Advanced SDV nella versione 1.4 i sistemi impiegati per il set up della eCRF dello Studio. ACTIDE è un sistema proprietario sviluppato e validato da Nubilaria, conforme ai requisiti di ICH E6 GCP e FDA 21 CFR Part 11 (MAC 006-005 - STUDY COMPLIANCE STATEMENT e MAC 015-014 –ACTideeCRF VERSION 2.3.9 - VALIDATION STATEMENT).
Nello specifico:

- MAC 006-005 - STUDY COMPLIANCE STATEMENT: attesta che la eCRF creata per lo studio è conforme ai sistemi sviluppati e validati da Nubilaria stessa.
- MAC 015-014 - ACTide ADVANCED SDV VERSION 1.4 - VALIDATION STATEMENT: è un estratto sintetico del risultato del processo di validazione del sistema informatico per il Sistema ACTide Advanced SDV - Versione 1.4, delle politiche di sicurezza e della conformità del sistema alle normative.

Software FMI
Cartelle dei pazienti in possesso alle Cliniche 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 Cabogen sono considerati specifici, espliciti e legittimi per diverse ragioni:

a) lo Studio Cabogen, condotto da GOIRC, è un'indagine scientifica finalizzata a comprendere le caratteristiche genomiche dei tumori e le relative opzioni terapeutiche; il trattamento dei dati è pertanto orientato a raggiungere obiettivi di ricerca chiaramente definiti e legittimi nel campo della ricerca oncologica;
b) uno degli scopi principali del trattamento dei dati è l'analisi della profilazione genomica tumorale; vengono analizzati i campioni di tessuto per identificare le mutazioni genomiche.

I dati raccolti saranno trattati esclusivamente per le finalità dello Studio, per la realizzazione del quale i dati saranno raccolti e inseriti in forma pseudonomizzata nelle e-CRF

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 ovvero non contattabili, nella procedura di consultazione preventiva ex art. 110 del Codice, unitamente al parere dei comitati etici, oltre che nell'art. 9, par. 2, lett. j) del Regolamento.

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.
Al fine di assicurare che i soggetti interessati dal trattamento dei dati personali ricevano un'adeguata informazione, viene predisposto dal GOIRC 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 per fini di ricerca dei dati personali dei pazienti. Il soggetto arruolato riceve pertanto due moduli distinti: consenso informato (relativo alla salute) e informativa/consenso (relativo alla privacy).

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 e dall'utilizzo di campioni di tessuto da nefrectomia o da un sito metastatico per eseguire il profilo genomico con un saggio di sequenziamento di nuova generazione "FoundationOne®CDx (F1CDx)" basato sulla cattura ibrida che permette di studiare le caratteristiche del DNA del tumore, in particolare analizzando 324 geni noti per essere associati al cancro.
L'analisi verrà eseguita in un singolo laboratorio certificato "Foundation Medicine", con sede a Penzberg in Germania.
Il campione di tessuto oggetto di analisi proviene dal blocchetto del campione tumorale del paziente, conservato in paraffina, che è stato prelevato al momento della diagnosi iniziale della malattia (tumore primitivo o metastasi). Il campione di tessuto è attualmente conservato presso l'anatomia patologica di ciascun centro clinico.
Al termine delle analisi il campione sarà restituito al centro clinico di provenienza.

2.4 I dati sono esatti e aggiornati?
I dati raccolti nello Studio Cabogen sono conformi e verificati per garantire la loro accuratezza e aggiornamento. Le Cliniche coinvolte 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.

2.5 Qual è il periodo di conservazione dei dati?
La durata massima del trattamento dei dati personali nello Studio è stabilita in due 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, l'analisi, la profilazione genomica tumorale 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 intervallo di tempo tiene conto dei tempi necessari per l'elaborazione dei dati, l'interpretazione dei risultati e la revisione scientifica.
Dunque, il periodo necessario per lo svolgimento ed il completamento dello studio, compreso il trattamento necessario per la finalità di ricerca scientifica, è di due anni mentre 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), è di sette annidopo il completamento della sperimentazione.
Tenuto conto di queste ragioni, si ritiene che i dati ed i campioni biologici 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.
Saranno messe in atto garanzie standardizzate per i trasferimenti di dati dalla CRO allo Sponsor.

Ecol Studio, al termine dello studio clinico e dopo aver proceduto al trasferimento dei dati pseudonimizzatiarchiviati sul database (eCRF su piattaforma ACTIDE) al GOIRC, procederà:

1. alla restituzione al GOIRC dei documenti pseudonimizzati di studio, in formato cartaceo ed elettronico, che contengono i dati di studio per l'archiviazione, a cura del GOIRC, nel Trial Master File o Archivio del Promotore;
2. alla richiesta di cancellazione al servizio IT, in ottemperanza al diritto di cui all' art. 17 del Regolamento nei confronti degli Interessati del trattamento, dei dati pseudonimizzati dai seguenti archivi:
   - server aziendali, inclusi quelli di backup e sicurezza;
   - dispositivi elettronici aziendali usati dai soggetti autorizzati al trattamento dei dati da Ecol Studio SpA;
   - caselle mail a cui hanno accesso i soggetti autorizzati al trattamento dei dati da Ecol Studio SpA;
3. alla richiesta di cancellazione dei dati pseudonimizzati, contenuti nel database utilizzato per l'attività di studio, al Sub-Responsabile del trattamento (NubilariaSrl) che ha partecipato all'attività di ricerca oggetto del contratto attraverso l'utilizzo del modulo "Final Decomissioning – Disposal Request".

Tale attività di cancellazione è da quest'ultimo eseguita in accordo alla SOP CDM 002 e documentata attraverso una apposita dichiarazione "Final Decomissioning – Disposal Confirmation" che dà evidenza dell'avvenuta distruzione e pulizia dei sistemi secondo appropriati standard di sicurezza.

In merito alla condivisione con il GOIRC dei dati finalizzati alla stesura del report statistico - redatto in conformità allo STROBE Statement (Checklist of terms that should be included in reports of observational studies - e/o di pubblicazioni, Ecol Studio procederà all'export dei dati pseudonimizzati, inseriti nel database clinico (e-CRF) allestito all'inizio dello studio in accordo alle indicazioni del Garante espresse nelle Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008 [1533155] secondo cui non vengono richiesti dati identificativi (quali data di nascita, iniziali, collocazione geografica) al fine di ridurre il rischio di consentire il riconoscimento dell'interessato.

Il trattamento dei dati da parte di Roche S.p.A. cessa al termine dello Studio CABOGEN, 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.

Roche S.p.A. si impegna a garantire che i propri sub-responsabili, FMI Germany GmbH e Foundation Medicine Inc., aderiscano a rigorose misure di sicurezza e privacy durante il trattamento dei dati all'interno dello Studio Cabogen. Roche assicura che entrambi i sub-responsabili effettueranno la distruzione completa dei dati al termine della propria attività, al fine di preservare la riservatezza e la protezione delle informazioni raccolte.

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.

Le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica stabiliscono inoltre che "Nel manifestare il proprio consenso ad un´indagine medica o epidemiologica, all'Interessato è richiesto di dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca" prevedendo specifiche modalità per la comunicazione di tali cd incidental findings agli interessati, al fine di assicurarne il rispetto della dignità nonché la tutela dell'autodeterminazione informativa degli stessi, anche in relazione al cd "*diritto di non sapere*"(art. 8).

Le Prescrizioni relative al trattamento dei dati genetici allegato n. 4 al Provvedimento 146 del 5 giugno 2019, che individua le prescrizioni contenute nelle Autorizzazioni generali che risultano compatibili con il Regolamento e con il D.lgs. n. 101/2018 di adeguamento del Codice, stabiliscono che:

"*Le informazioni da rendere agli interessati debbano dare evidenza:*

a) dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;

b) *della facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi."*

In accordo a tali disposizioni, nel Foglio Informativo e Consenso allo studio è prevista la possibilità per il paziente di scegliere se essere informato o meno o se rendere disponibili ai familiari informazioni in merito ai risultati delle indagini genetiche in presenza di *incidental findings*.

I Centri partecipanti effettueranno ogni ragionevole sforzo per contattare tutti i pazienti che soddisfano i criteri di idoneità all'arruolamento allo Studio, 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 i pazienti che dovessero risultare deceduti o non rintracciabili, l'esecuzione dei necessari tentativi per contattare/rintracciare i pazienti sarà documentata dallo Sperimentatore Principale attraverso la compilazione e sottoscrizione di un Modulo di Dichiarazione Sostitutiva al Consenso.

Verranno, inoltre, adottate idonee forme di pubblicità dell'informativa, ex art. 14 del Regolamento e ex art. 6 della Regole Deontologiche, mediante diffusione di "Informativa Pubblica" presso 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.

GOIRC si impegna altresì a fornire ai pazienti deceduti o non più contattabili un'adeguata informativa riguardo alla promozione dello Studio Cabogen; le informazioni ai pazienti deceduti o non più contattabili (rispetto ai quali non è possibile richiedere il consenso al trattamento dei dati) saranno fornite, ai sensi dell'art. 14, par. 5, lett. b) del Regolamento e dell'art. 6 delle Regole deontologiche, mediante pubblicazione sui siti del Promotore e dei centri partecipanti, in sezioni facilmente accessibili e "per l'intera durata dello Studio", assicurando che gli interessati ed i loro aventi causa, pur non avendo un contatto diretto con il Titolare e Promotore dello Studio, possano conoscere, in modo agevole, i trattamenti dei propri dati.

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

GOIRC 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 Cabogen e 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 al massimo intorno al 50%, circa 40 pazienti su 80. Questo a causa dell'elevata incidenza della mortalità per la patologia oggetto dello Studio, nonché dell'eventualità che i pazienti non facciano più ritorno al Centro per motivi di follow up, essendo inclusi nel campione pazienti in stadio avanzato della malattia e tenuto conto del periodo di tempo trascorso dal momento in cui i dati riferiti agli Interessati sono stati originariamente raccolti.

2.7 Come si ottiene il consenso degli interessati?

Al fine di assicurare che i soggetti interessati dal trattamento dei dati personali ricevano un'adeguata informazione, viene predisposto dal GOIRC 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 per fini di ricerca dei dati personali dei pazienti.

Per i pazienti che dovessero risultare deceduti o non rintracciabili, l'esecuzione dei necessari tentativi per contattare/rintracciare i pazienti sarà documentata dallo Sperimentatore Principale attraverso la compilazione e sottoscrizione di un Modulo di Dichiarazione Sostitutiva al Consenso.

Verranno, inoltre, adottate idonee forme di pubblicità dell'informativa, ex art. 14 del Regolamento ed ex art. 6 delle Regole Deontologiche, mediante diffusione di "Informativa Pubblica" 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.

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

Nel foglio informativo e modello di consenso al trattamento predisposto dal GOIRC 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 responsabile 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 Cabogen 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)?

Nel foglio informativo e modello di consenso al trattamento predisposto dal GOIRC 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 responsabile 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.

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 originalmente 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.

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

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

Nel foglio informativo e modello di consenso al trattamento predisposto dal GOIRC 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 responsabile 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 Cabogen e di esercitare i propri diritti se lo desiderano.

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

Per la realizzazione dello Studio, il GOIRC in qualità di titolare si avvale del supporto di responsabili esterni e sub-responsabili esterni come specificato al punto 1.2 della presente VIP; 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.
Inoltre, i rapporti tra i responsabili del trattamento e i sub-responsabili sono anch'essi regolati contrattualmente; i sub-responsabili esterni, come specificati nel punto 1.2 del presente Documento di Valutazione dell'Impatto sulla Protezione dei Dati (DPIA), hanno sottoscritto contratti con i rispettivi responsabili.

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

Nel caso di trasferimento di dati al di fuori dell'Unione Europea, è garantita una protezione equivalente. Nel contesto dello Studio Cabogen, il trasferimento fuori dall'Unione europea avviene per i dati trasferiti tra Roche e il proprio sub-responsabile Foundation Medicine Inc. poiché Foundation Medicine ha sede negli Stati Unitiil trasferimento dei dati è legittimato dalla decisione di adeguatezza adottata il 10 luglio 2023 dalla Commissione europea.
Inoltre, il trasferimento di dati personali tra Roche e Foundation Medicine Inc. è regolato dall'utilizzo di clausole contrattuali standard, conformi alle decisioni dell'Unione Europea in materia di trasferimento di dati personali verso paesi terzi.
Le clausole contrattuali standard stabiliscono obblighi giuridicamente vincolanti per le parti coinvolte, al fine di garantire la sicurezza e la protezione dei dati personali trasferiti. Esse includono disposizioni sulla riservatezza, l'uso limitato dei dati personali, la sicurezza dei dati e i diritti degli interessati.
Pertanto, attraverso l'adozione di clausole contrattuali standard tra Roche e Foundation Medicine Inc., il trasferimento di dati personali è sottoposto a meccanismi di protezione adeguati ed equivalenti a quelli richiesti dal GDPR. Ciò assicura che i diritti degli interessati siano rispettati e che i dati personali siano trattati in conformità alle normative vigenti sulla protezione dei dati.

3. RISCHI

3.1 Misure di sicurezza esistenti e pianificate

L'attività sarà svolta presso ognuno dei 12centri, 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 e dai referti del test di profilazione genomica, eseguiti da Roche S.p.a. tramite lo strumento "FoundationOne®CDx (F1CDx)" sui campioni di tessuto dei pazienti.
Tali dati saranno inseriti all'interno di un database elettronico (eCRF), con modalità di Remote Data Entry, 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 del presente studio. I dati verranno inseriti all'interno della CRF previa pseudonimizzazione e ogni paziente sarà identificato solo attraverso un codice numerico.
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 (Sperimentatori, Ricercatori, Clinical Monitor).

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

Non sono previsti dati provenienti da fonti esterne (es. risultati di analisi di laboratorio centralizzato) da immettere in eCRF in modo automatico.

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

Dopo la chiusura del database e poco prima della rimozione dello stesso, tutti i dati raccolti in eCRF saranno consegnati al GOIRC su idoneo supporto magnetico oppure trasferiti mediante piattaforma di condivisione file tramite web o altre modalità, con le opportune protezioni e saranno conservati dal GOIRC in un luogo protetto per il tempo necessario al perseguimento degli scopi della raccolta.

Prima della consegna, i file saranno compressi e protetti da password e la password sarà comunicata al GOIRC a parte, in forma scritta. Il ricevimento e la corretta leggibilità dei file saranno documentati.

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 è installato su server dedicati presso la server farm Aruba S.p.a., dotata di sistema per la gestione qualità certificato ISO 9001:2015, di sistema per la gestione della sicurezza delle informazioni certificato ISO 27001:2013 e di sistema per la gestione dei data center certificato ANSI/TIA-942-A.

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

Dopo la chiusura del database, si procederà con l'estrazione degli export dei dati pseudonimizzati e il loro trasferimento al GOIRC che procederà all'esecuzione di un'analisi statistica di tipo descrittivo che avrà ad oggetto:

- il profilo genomico dei pazienti e le caratteristiche basali come peso, ECOG PS, classificazione del punteggio IMDC, siti di metastasi, risposta a precedenti trattamenti in base al profilo genomico dei pazienti.
- la sopravvivenza globale calcolata dalla data di inizio del trattamento fino alla data di morte per qualsiasi causa o data dell'ultimo contatto in caso di censura.
- durata della risposta calcolata come il tempo dalla documentazione della risposta del tumore alla progressione della malattia.
- risposta complessiva: considerata come la percentuale dei pazienti con Complete Response (CR) e Partial Response (PF).

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

Per lo svolgimento delle attività legate allo sviluppo e al mantenimento della eCRF, la CRO si avvarrà di una terza parte, la società NubilariaSrl con sede legale in Italia, nominata sub responsabile del trattamento.

La Società NubilariaSrl svolgerà in particolare attività di noleggio e manutenzione della piattaforma ACTIDE, hosting dei dati in server dedicati e noleggio di linee certificate di trasmissione dei dati. L'attività svolta è dunque di natura meramente tecnica, Nubilaria non ha alcun ruolo attivo nella raccolta dei dati che saranno quindi trattati come di seguito indicato.

I pazienti sono pseudonimizzati by design, ACTide assegna un codice paziente univoco e Nubilaria non è in possesso di documentazione con dati identificativi dei pazienti.

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 ACTIDE. 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 dalla CRO Yghea. Fuori da tali ipotesi, i dati saranno trattati solo in forma pseudonimizzata o aggregata e non saranno diffusi a soggetti diversi dal GOIRC, dai Centri e dalla CRO per le finalità della conduzione dello Studio.
Roche tratta i dati personali principalmente utilizzando modalità informatiche. In particolare, i dati vengono trattati mediante l'invio di dati pseudonimizzati al responsabile esterno (Roche) che utilizza i propri strumenti hardware e software per condurre le attività di trattamento.
Roche S.p.A. si impegna a trattare i dati personali solo per le finalità previste nel contesto dello Studio CABOGEN e si astiene dall'utilizzare tali dati per altri scopi come anche specificamente indicato nella nomina a responsabile esterno del trattamento. I dati vengono principalmente trattati in forma elettronica attraverso l'invio di dati pseudonimizzati ai sub-responsabili esterni designati, rispettando i requisiti di sicurezza e privacy applicabili.
Per garantire la sicurezza dei dati personali, Roche S.p.A. attua adeguate misure di sicurezza tecniche e organizzative per prevenire accessi non autorizzati, la divulgazione, l'alterazione o la distruzione dei dati. Tali misure sono state sottoposte a audit da parte di GOIRC e includono il controllo dell'accesso ai dati da parte di personale autorizzato, l'utilizzo di pseudonimizzazione per proteggere i dati in transito e in archivio, la gestione dei backup dei dati e l'adeguata formazione del personale coinvolto nel trattamento dei dati.
Roche S.p.A. ha a sua volta stabilito contratti di sub-responsabilità e ha adottato misure appropriate per regolare il trasferimento di dati personali con i suoi sub-responsabili esterni: FMI Germany GmbH e Foundation Medicine Inc. con la quale ha stipulato specifiche clausole contrattuali standard come previsto dalla normativa in materia di protezione dei dati. Per il trasferimento dei dati tra Europa e USA è inoltre in vigore la recente decisione di adeguatezza adottata il 10 luglio 2023 dalla Commissione europea.

3.2 Accesso illegittimo ai dati

Se il rischio di accesso illegittimo ai dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli interessati come di seguito riportati.
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, come ad esempio per attività di frode o 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 Cabogen, compromettendo l'efficacia dello studio.
L'accesso illegittimo ai dati potrebbe avere conseguenze legali con azioni legali avanzate da parte degli Interessati, oltre a multe o sanzioni da parte del Garante a seguito di una violazione della normativa sulla protezione dei dati.

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 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 e nella documentazione fornite dal titolare ai responsabili esterni.

a) Accesso limitato e controllato ai dati personali del solo personale autorizzato sia a livello fisico che informatico.
b) Pseudonimizzazione dei dati e la 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, sub-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 e sub-responsabili.

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

Sebbene la sensibilità dei dati trattati sia elevata, il numero di interessati coinvolti è limitato a circa 80 pazienti. Considerando gli 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.

3.2.5Come 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 Cabogen, portando a conclusioni errate o inesatte.

Le Cliniche, lo Sponsor e soprattutto i pazienti interessati potrebbero perdere fiducia nella correttezza e nell'integrità dei dati personali raccolti e trattati nello studio. 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 Cabogen. 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, possono 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 e nella documentazione fornita dal titolare dai responsabili esterni.

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) Implementazione di 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 possano 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 e sub-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.

3.3.5Come 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

Se il rischio di perdita dei dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli interessati come di seguito riportati:

Gli interessati potrebbero subire la perdita permanente delle proprie informazioni personali relative a dati sensibili come informazioni mediche e analisi cliniche, inoltre l'intero Studio sarebbe compromesso.

La perdita di dati potrebbe comportare conseguenze legali per lo Studio Cabogen e per i responsabili del trattamento dei dati. Gli interessati potrebbero intraprendere azioni legali per richiedere riparazioni o risarcimenti per il danno subito a seguito della perdita dei propri dati personali.

Gli interessati potrebbero sperimentare disagio, preoccupazione e stress emotivo a causa della perdita dei propri dati personali.

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:

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.
f)

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 e nella documentazione fornita dal titolare dai responsabili esterni.

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.

3.4.5Come 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.

Gruppo Oncologico Italiano di Ricerca Clinica - GOIRC
in persona del presidente del Consiglio Direttivo
Prof. Antonino Musolino

Firmato digitalmente da: ANTONINO MUSOLINO
Data: 14/12/2023 17:19:27