CNAO
Centro Nazionale di Adroterapia Oncologica

Via Erminio Borloni, 1 27100 PAVIA
Tel. 0382 0781 – www.cnao.it

Numero	*Data*	*Rev.*	*Pagina*
DOC-SD-NT-GEN-00277_estratto	27.05.2025	0	1 di 21

Documento tipo / Document type

NOTA TECNICA

Titolo / Title

Valutazione di Impatto sulla Protezione dei Dati (DPIA) per le attività di Ricerca Clinica (estratto per pubblicazione sul sito cnao.it)

Autori (CNAO se non diversamente indicato) / Authors (CNAO if not differently indicated)

N. Facchinetti, C. Bono, A. Ferent, V. Ghio, M. Russo, L. Licitra

Referente / Contact person

N. Facchinetti

Parole chiave / Keywords

Studi clinici, dati personali, gestione dei dati, GDPR

Riassunto / Abstract

Il presente documento rappresenta un estratto della revisione della DPIA per le attività di ricerca clinica pubblicata in data 27.04.2020 (NTECC-NGPRI-00016) ed esprime i risultati della valutazione del rischio e di impatto sui diritti e le libertà delle persone in riferimento ai processi di ricerca clinica sulle applicazioni dell'adroterapia per la Fondazione CNAO.
Alcune informazioni contenute nella versione integrale sono state rimosse o riassunte per salvaguardare il know-how aziendale, come consentito dall'Autorità Garante per la Protezione dei Dati Personali. Le omissioni sono indicate con la dicitura "[...omissis...]".
Il documento completo, contenente tutte le informazioni dettagliate è messo a disposizione delle Autorità competenti su richiesta, nel rispetto degli obblighi di trasparenza previsti dalla normativa vigente.

Emesso / Compiled	*Verificato / Controlled*	*Verificato / Controlled*	*Approvato / Approved*
N. Facchinetti, C. Bono, A. Ferent, V. Ghio, M. Russo	**L. Licitra**	**C. Delaini**	**S. Rossi**
	LISA FRANCESCA LINDA LICITRA 11.06.2025 14:36:40 GMT+01:00	Firmato digitalmente da: CHIARA DELAINI Data: 12/06/2025 21:30:43	SANDRO ROSSI 13.06.2025 11:31:38 GMT+01:00

LISTA DI DISTRIBUZIONE / DISTRIBUTION LIST			
#	*Data / Date*	*Nome / Name*	*Ditta / Society*

ELENCO DELLE VARIAZIONI / HISTORY OF CHANGES			
Ver.	*Data / Date*	*Pag.*	*Descrizione / Description*
0	27.05.2025	21	Nuova emissione a valle della revisione base giuridica del trattamento e misure di sicurezza

INDICE

1 PREMESSE

La **Valutazione d'Impatto sulla Protezione dei Dati** (di seguito "**DPIA**") è un processo che ogni Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone, in particolare se connesso all'impiego di nuove tecnologie.

1.1 CONTESTO GENERALE DI APPLICAZIONE

CNAO - Centro Nazionale di Adroterapia Oncologica è un istituto di eccellenza dedicato alla cura dei tumori mediante l'adroterapia, una tecnica all'avanguardia nell'ambito della radioterapia oncologica. Oltre alla sua missione clinica, CNAO si distingue per il suo impegno nella ricerca scientifica e clinica, promuovendo e realizzando progetti con l'obiettivo di migliorare costantemente l'offerta terapeutica.

La ricerca clinica, parte integrante delle attività del Centro, mira a determinare, su soggetti umani, la sicurezza e l'efficacia di ogni approccio clinico, inclusi dispositivi, prodotti diagnostici, farmaci o soluzioni innovative, comprese combinazioni di questi. Tale ricerca abbraccia pratiche preventive, diagnostiche e terapeutiche, strettamente collegate allo sviluppo e all'ottimizzazione della stessa, nel pieno rispetto delle **Good Clinical Practices (GCP)** e degli standard, delle norme, delle linee guida, nazionali ed internazionali, vigenti per la ricerca clinica, sia su farmaco che su dispositivo.

L'attività di ricerca clinica del CNAO si esplica sostanzialmente attraverso tre tipologie:

- **Ricerca Osservazionale Retrospettiva**: studio clinico che non ha impatti diretti sulla terapia del paziente, ma è basato solo su raccolta retrospettiva e analisi di dati raccolti nell'ambito della terapia standard (in riferimento a quanto disposto dall' art. 2, par. 2, n. 4, Regolamento UE 2014/536);
- **Ricerca Osservazionale Prospettica**: studio clinico che non ha impatti diretti sul processo di cura, ma è basato solo sui dati derivanti dalla normale pratica clinica e le osservazioni avvengono progressivamente nel tempo, seguendo il paziente nel suo percorso clinico. (in riferimento a quanto disposto dall' art. 2, par. 2, n. 4, Regolamento UE 2014/536);
- **Ricerca Interventistica**: studio clinico, con dispositivo medico e/o di ottimizzazione del trattamento adroterapico e/o farmacologico, che soddisfa una delle seguenti condizioni:
  a. l'assegnazione del soggetto a una determinata strategia terapeutica è decisa anticipatamente e non rientra nella normale pratica clinica;
  b. la decisione di prescrivere i medicinali sperimentali o l'uso del dispositivo fuori dalla normale pratica clinica e la decisione di includere il soggetto nello studio clinico sono prese nello stesso momento;

  In questa categoria rientrano anche le procedure diagnostiche o di monitoraggio aggiuntive rispetto alla normale pratica clinica (in riferimento a quanto disposto dall' art. 2, par. 2, n. 2, Regolamento UE 2014/536; art. 2, par. 45, Regolamento UE 2017/745).

2 OGGETTO DEL DOCUMENTO

Il presente documento descrive l'attività di Valutazione d'Impatto (**DPIA**) svolta per la conduzione di studi **osservazionali**, sia **retrospettivi** che **prospettici**, e di studi **interventistici**, inclusi quelli a **bassa intensità**. Gli studi presi in considerazione possono essere **monocentrici**, ossia condotti esclusivamente presso il CNAO, o **multicentrici**, cioè realizzati in più centri di ricerca o strutture sanitarie coordinate tra loro per raccogliere e analizzare dati in modo integrato.

Il documento si riferisce a tali sperimentazioni/studi sia nel caso in cui CNAO svolga il ruolo di **Promotore**, assumendosi la responsabilità (dalla pianificazione alla conduzione, al monitoraggio fino all'interpretazione e alla diffusione dei risultati), sia nel caso in cui operi come **Centro Partecipante**, contribuendo alla raccolta e gestione dei dati secondo il protocollo definito dal Promotore.

3 DOCUMENTI COLLEGATI

RIFERIMENTO	SCOPO DEL DOCUMENTO
P-P02	Progettazione e gestione della ricerca clinica
P-F01	Gestione del sistema informatico aziendale
IST-CT-MOI-001	Pseudonimizzazione e anonimizzazione dati studi clinici
Mod. 040	Dati di Base Progetto – Ricerca Clinica
Mod. 041	Piano di Progettazione
Mod. 085	Consensi e informative sull'uso dei dati dei pazienti per attività di ricerca osservazionale nel registro REGAL
Mod. 255	Study Specific Delegation of Authority Log
Mod. 256	Template protocollo di studi clinici interventistici
Mod. 257	Template protocollo di studi osservazionali
Mod. 258	Notifica raccolta dati retrospettivi
Mod. 261	Modulo Informativo per la Partecipazione allo Studio Osservazionale
Mod. 262	Foglio Informativo e Consenso Informato alla partecipazione allo studio interventistico
Mod. 270	Consenso Informato per prelievo e stoccaggio di Materiale Biologico
Mod. 497	Tabella di transcodifica studio osservazionale
Mod. 516	Monitoring Visit Report
Mod. 518a	Consenso per il trattamento dei dati e partecipazione allo studio osservazionale
Mod. 518b	Consenso per la partecipazione sperimentazione clinica interventistica
Mod. 548	Modulo di revoca del consenso alla partecipazione allo studio

4 DESCRIZIONE DEL TRATTAMENTO

4.1 TRATTAMENTO OGGETTO DI VALUTAZIONE

Il trattamento oggetto di valutazione riguarda la **ricerca clinica**, che include sia attività di natura osservazionale sia interventistica. Tali attività mirano a produrre conoscenze che **possono,** nell'immediato o in un prossimo futuro, **avere un impatto sullo stato di salute dei pazienti**.

In particolare, la ricerca **osservazionale** si concentra sulla raccolta e analisi di dati **senza intervenire direttamente sui soggetti arruolati**, mentre la ricerca **interventistica** prevede l'introduzione di pratiche mediche finalizzate ad accertare la sicurezza e/o l'efficacia di determinati interventi, con un **potenziale impatto diretto** sullo stato di salute, sulla vita o sul benessere dei **partecipanti**.

All'interno del presente documento vengono analizzati i **rischi** connessi al trattamento di dati personali nell'ambito delle attività di ricerca clinica sopra introdotte e sono illustrate le **misure tecniche ed organizzative** adottate dal CNAO per minimizzare tali rischi.

4.2 DATI PERSONALI RACCOLTI, TRATTATI E LORO CICLO DI VITA

In ogni studio clinico, CNAO si impegna a raccogliere unicamente i **dati pertinenti e necessari** per svolgere le attività di ricerca descritte nel protocollo nel pieno rispetto del **principio di minimizzazione**.

Il principio di minimizzazione dei dati è garantito dalla **applicazione rigorosa del protocollo clinico** di ogni studio, che individua esattamente le aree di indagine e quindi le informazioni necessarie per la realizzazione dello studio. Nelle eCRF sono raccolti esclusivamente i dati indicati richiesti dal protocollo clinico e finalizzati al raggiungimento dell'obiettivo dello studio.

Considerando le possibili tipologie di dati legati alla patologia in oggetto ed agli obiettivi dello studio, di seguito si propone una **classificazione generica** dei dati personali raccolti per lo svolgimento di tali ricerche nelle categorie previste dal GDPR, ricostruita da un campione di studi clinici condotti in CNAO. **L'elenco che segue non ha la pretesa di essere esaustivo**, considerando che nuove tecnologie e continui progressi in ambito scientifico potrebbero in futuro consentire la raccolta e l'utilizzo di nuove informazioni oggi inaccessibili. Si è tuttavia ritenuto opportuno considerare la gamma più ampia possibile di dati personali generalmente trattati negli studi, soprattutto ai fini del calcolo del rischio iniziale per i diritti e le libertà dei pazienti arruolati associabile ai trattamenti effettuati.

La definizione specifica di quanti e quali dati siano necessari per ogni studio è presente nel protocollo clinico.

DATI PERSONALI PROCESSATI NELLA RICERCA CLINICA	
DATI COMUNI	**Dati identificativi e anagrafici** Esempi: nome, cognome, codice fiscale, sesso, età, … **Dati di contatto** Esempi: indirizzo e-mail e numero di telefono **Dati relativi allo stile di vita** Esempi: peso, altezza, alimentazione, …
DATI RICONDUCIBILI A "CATEGORIE PARTICOLARI"	**Dati relativi allo stato di salute** Esempi: età, diagnosi, istologia del tumore, trattamenti ricevuti nel tempo, TC, RM, comorbidità …
	Biomarcatori (contenenti anche i dati genetici) Esempi: biomarcatori diagnostici, prognostici e predittivi, di natura omica
	Campioni biologici Esempi: sangue, campioni bioptici, saliva, urine…
	Dati relativi alla vita sessuale Esempi: uso di anticoncezionali, gravidanze, …
	Dati relativi all'origine razziale o etnica Esempi: Etnia, …
	Convinzioni religiose NA

I dati sopra elencati sono trattati unicamente dai **soggetti** appositamente **autorizzati secondo le procedure interne di CNAO** e definiti per ogni studio all'interno del Delegation of Authority Log (Mod. 255) o nel Registro dei Trattamenti.

In particolare, sono soggetti autorizzati da CNAO a trattare i dati personali dei partecipanti a studi clinici:

- Medici e professionisti (fisica medica, bioingegneria, radiobiologia, TSRM…) incaricati della prestazione sanitaria (per la produzione dei source documents);
- Principal Investigators (PI) dei singoli progetti di ricerca;
- Membri del team di ricerca dei PI (per la raccolta dei dati dai source documents e la loro elaborazione ed analisi);
- Clinical Trials Center (per la raccolta dei dati dai source documents e/o da questionari, loro elaborazione ed analisi)
- Personale dei sistemi informativi e/o dei fornitori dei servizi di assistenza e manutenzione ai software, per le sole attività di manutenzione dei sistemi.

La garanzia di esattezza e aggiornamento dei dati è garantita dall'esecuzione del protocollo clinico. I dati del partecipante sono periodicamente aggiornati per tutta la durata dello studio fino al termine delle procedure descritte nel protocollo.

Per gli studi retrospettivi, l'esattezza dei dati è relativa al momento in cui gli stessi sono stati raccolti, così come conservati in cartella clinica e nei software del CNAO, e non c'è necessità di aggiornamento.

L'intero ciclo di vita dei dati dei partecipanti allo studio clinico, con particolare attenzione ai ruoli e alle responsabilità dei soggetti coinvolti, è descritto in dettaglio all'interno della Procedura P-P02 (Procedura per la gestione della ricerca clinica).

4.3 SOGGETTI COINVOLTI E RESPONSABILITÀ

Il titolare del trattamento è il promotore dello studio clinico, generalmente ne sono contitolari gli eventuali Centri Sperimentatori coinvolti (nel caso di sperimentazioni multicentriche).

Di conseguenza, quando è promotore di un progetto di ricerca clinica, il CNAO agisce in qualità di Titolare del Trattamento. Quando invece è centro di sperimentazione non promotore (coinvolto in uno studio clinico multicentrico), il CNAO agisce – generalmente - in qualità di contitolare del trattamento del Promotore. Questa situazione viene comunque valutata caso per caso.

I dati trattati da **CNAO** per il perseguimento delle finalità di ricerca sono trasmessi o eventualmente acceduti ai soggetti coinvolti a vario titolo nella sperimentazione, in funzione del ruolo e del tipo di studio, quali:

- **Autorità sanitarie competenti**: Istituzioni preposte alla valutazione e verifica della conformità dello studio per le materie di propria competenza;
- **Sponsor**: Promotore dello Studio nei casi di studi multicentrici;
- **Enti partner dello studio**: Centri sperimentatori o istituzioni universitarie coinvolte nel caso di studi multicentrici;
- **CRO** (Clinical Research Organization): Fornitore eventualmente incaricato di gestire e coordinare le attività di ricerca, nominato responsabile del trattamento (anche nella ricerca osservazionale);
- **Laboratori di analisi**: Fornitori eventualmente incaricati di svolgere analisi di campioni biologici, nominati responsabili del trattamento;

- **Provider di servizi, app o software in cloud**: Fornitori incaricati di svolgere attività di messa a disposizione e manutenzione di infrastrutture, soluzioni tecnologiche o archivistiche e nominati responsabili del trattamento.
- Medico di medicina generale: se del caso all'interno di studi interventistici.

L'attività di terapia effettuata dal CNAO e la gestione della relativa documentazione clinica è effettuata sotto la esclusiva responsabilità del CNAO, in qualità di Titolare del Trattamento, in un processo separato che alimenta quello della ricerca clinica.

4.4 RISORSE DI SUPPORTO AI DATI

I dati di ogni studio clinico sono gestiti secondo le regole e le misure stabilite nel protocollo clinico e secondo i requisiti minimi di sicurezza fissati nella P-P02.

5 VALUTAZIONI IN ORDINE ALLA NECESSITÀ E ALLA PROPORZIONALITÀ DEI TRATTAMENTI

5.1 SCOPO E BASE GIURIDICA DEL TRATTAMENTO

RICERCA OSSERVAZIONALE

Per la tipologia di ricerca osservazionale, ai sensi del parere dell'EDPB del 02/2021 (punto 12), del dettato del D. Lgs. 196/03 e delle espressioni del Garante per la Protezione dei Dati, CNAO ha adottato come fondamento di liceità generale il **consenso esplicito dell'interessato**, trattandosi di ricerca svolta puramente sui dati, senza alcun intervento sull'individuo.

In particolare, a partire dal 2021, CNAO conduce un registro ambispettico chiamato "REGAL" (CNAO OSS 25 2021- NCT05203250), gestito nei sistemi informativi interni, contenente i dati clinici, fisici, dosimetrici e di valutazione del benessere psicofisico dei pazienti della Fondazione. In linea con gli obiettivi dello studio, il registro viene utilizzato nella ricerca per generare dati clinici volti ad aumentare le conoscenze sull'adroterapia. I dati ed i documenti (es. immagini o referti) oggetto di ricerca che compongono il registro sono quelli raccolti durante le valutazioni cliniche e/o il trattamento adroterapico.

REGAL costituisce una base dati per molti degli studi osservazionali condotti in CNAO. I dati ivi contenuti possono essere utilizzati sia per sotto-analisi che per analisi specifiche previa stesura di un protocollo clinico redatto in conformità alla normativa e alle linee guida vigenti. È compito del PI definire se il disegno di studio sia in linea con gli obiettivi e i dati raccolti all'interno di REGAL.

Premesso quanto sopra, il trattamento dei dati personali a scopo di ricerca osservazionale è effettuato solo nei seguenti casi:

1. Il paziente ha rilasciato il proprio **consenso per l'inserimento dei propri dati personali all'interno del registro REGAL** (comprese le immagini, i referti ed ogni documento pertinente alla terapia). Questi dati possono essere pertanto utilizzati per le analisi dello studio REGAL e di tutte le sue sotto-analisi che, in linea con gli obiettivi dello stesso, sono finalizzati ad aumentare le conoscenze sull'adroterapia.
2. Il paziente ha rilasciato un **consenso studio-specifico** per uno studio osservazionale la cui indagine non rientra nel perimetro dello studio REGAL.

3. Il **soggetto** che si intende includere nello studio risulta **non reperibile** (perché deceduto o non più rintracciabile) e il PI, col supporto del CTC, ha compilato apposita documentazione in cui giustifica l'irraggiungibilità e la necessità di utilizzare tali dati ai fini della ricerca (Mod. 258).

Per i casi sopra descritti, è sempre il medico a somministrare al paziente o a chi ne esercita la potestà legale (laddove reperibile) l'informativa e il consenso in sede o da remoto attraverso un portale elettronico dedicato.

I dati così coperti da consenso possono essere utilizzati, previa pseudonimizzazione o anonimizzazione, dai ricercatori, sia del CNAO che di soggetti esterni con cui il CNAO collabora per il singolo studio dopo parere favorevole delle Autorità Regolatorie. L'operazione di pseudonimizzazione o anonimizzazione è a carico del CNAO (secondo la relativa istruzione operativa IST-CT-MOI-001) o di enti terzi, ove previsto.

I dati non coperti da consenso o, nel caso di soggetti non reperibili, dal Mod. 258, non possono essere utilizzati per la ricerca.

RICERCA INTERVENTISTICA

Nel caso di svolgimento di sperimentazioni e/o indagini cliniche il fondamento di liceità al trattamento più opportuno individuato dal CNAO consiste nella **esecuzione del contratto tra le parti, ex art. 6, 1° comma, lett. b) del Regolamento UE 2016/679**, poiché l'adesione spontanea ad uno studio clinico interventistico implica, necessariamente, il trattamento dei dati personali dei pazienti alla stregua di un processo di terapia **per finalità di assistenza o terapia sanitaria ai sensi dell'articolo 9 comma 2 lettera h) del Regolamento UE 2016/679**.

Come specificato dallo stesso EDPB – European Data Protection Board (paragrafi 5 e ss del documento di FAQ citato nei riferimenti normativi) e dall'articolo 28 comma 1 lettera d) del Regolamento sulle sperimentazioni cliniche, la presenza di un consenso informato espresso dal paziente per la partecipazione ad un progetto di ricerca clinica è un requisito diverso ed ulteriore rispetto alla definizione del fondamento di liceità del trattamento dei dati: l'adesione spontanea ad uno studio clinico interventistico implica, necessariamente, il trattamento dei dati personali del paziente (in esecuzione del contratto ai sensi dell'articolo 6 comma 1 lettera b) del GDPR) alla stregua di un processo di terapia secondo la normale pratica clinica (e quindi la legittimità del trattamento per finalità di assistenza o terapia sanitaria ai sensi dell'articolo 9 comma 2 lettera h) del GDPR).

Quindi, il paziente che aderisce alla sperimentazione o indagine clinica esprimendo chiaramente la sua volontà di partecipare non presta alcun consenso all'uso dei suoi dati, che è necessario per la realizzazione dello studio. Riceve tuttavia informazioni specifiche anche in materia di trattamento dei dati (sia in termini di finalità che di modalità) nel modulo informativo e nel modulo di consenso informato alla partecipazione allo studio, somministrati dal PI o delegato, e può liberamente decidere se aderire o meno al programma di ricerca sapendo che uso sarà fatto dei suoi dati e per quanto tempo. Qualora fosse prevista la raccolta di campioni biologici a scopo di ricerca, un ulteriore modulo per il consenso informato per prelievo e stoccaggio di materiale biologico verrà somministrato al paziente, che potrà volontariamente concedere o negare il consenso.

I dati così acquisiti possono essere utilizzati solo per la realizzazione dello studio clinico (ed essere eventualmente utilizzati solo a fini registrativi nel rispetto delle disposizioni vigenti).

I dati raccolti possono essere utilizzati dagli sperimentatori del CNAO e condivisi con gli altri soggetti autorizzati, sull'apposito sistema informativo designato nel protocollo e/o nel contratto di collaborazione, dopo essere stati pseudonimizzati o anonimizzati correttamente.

Qualora lo Sperimentatore Principale intendesse acquisire i dati della singola sperimentazione anche con lo scopo di riutilizzo dei dati per finalità di ricerca clinica ulteriore (cd. "riuso"), è tenuto a richiedere il consenso al paziente per l'inserimento in REGAL o in uno specifico studio osservazionale che coinvolga dati ulteriori rispetto a REGAL.

5.2 PERIODO DI CONSERVAZIONE DEI DATI

Il periodo di conservazione è stabilito in ogni singolo protocollo in funzione di ogni studio e, in ogni caso:

- per gli studi interventistici non superiore a 25 anni, come previsto dall'art. 58 del Regolamento (UE) 536/2014 sulla sperimentazione clinica di medicinali per uso umano;
- Per le indagini cliniche almeno 10 anni dalla fine della sperimentazione e se immesso in commercio, dai 10 ai 15 anni dalla data di immissione sul mercato a seconda del caso (Regolamento (UE) 2017/745).
- Per gli studi osservazionali, minimo 7 anni e massimo 50 (nel caso di studi incentrati su pazienti pediatrici e/o tumori rari) dal termine dello studio.

5.3 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Per ciascuno studio, i pazienti vengono debitamente informati dal PI o da un medico indicato nel delegation log circa le modalità e le finalità della ricerca, e vengono loro somministrati l'informativa, il consenso al trattamento dei dati personali (laddove previsto), oltre che il consenso informato alla partecipazione allo studio.

I diritti esercitabili dal paziente arruolato sono indicati nel modulo informativo.

[...omissis...]

5.4 FORMALIZZAZIONE DEI CONTRATTI

I responsabili del trattamento coinvolti nei processi di ricerca clinica, tipicamente il promotore o un altro centro sperimentatore che mette a disposizione il sistema informativo per le elaborazioni o una CRO, sono vincolati per contratto stipulato ai sensi dell'art. 28 del Regolamento UE 2016/679.

Come indicato nella P-P02, qualora il CNAO dovesse avvalersi di sistema informativo non proprio, o di prestazioni di analisi in service o di una CRO, nel contratto con la struttura individuata sono espressamente indicati i compiti affidati al responsabile del trattamento, le misure di sicurezza da garantire ed adottare, la finalità del conferimento dei dati, la durata del trattamento ed ogni altro obbligo da imporsi secondo lo specifico incarico conferito.

5.5 TRASFERIMENTI EXTRA SEE

In relazione alle operazioni di trattamento in esame, quando CNAO è il Promotore dello studio non è previsto il trasferimento di dati in Paesi Extra UE.

Come indicato nella P-P02, nei casi in cui il promotore o un centro partecipante si trovi in un paese fuori dallo SEE (Spazio Economico Europeo) è necessario che il contratto con l'ente promotore contempli la presenza di una decisione di adeguatezza o l'adozione delle clausole contrattuali standard approvate dalla Commissione Europea, nei casi di controller to controller.

6 ANALISI DEI RISCHI E DELLE MISURE DI SICUREZZA

6.1 METODOLOGIA DI VALUTAZIONE DEL RISCHIO

La valutazione del rischio per i diritti e le libertà delle persone è effettuata dai membri del Gruppo per la Protezione dei Dati, con la supervisione ed il parere del DPO, e formalizzata nel registro dei trattamenti.

La presente valutazione di impatto sui processi di ricerca clinica è stata effettuata, coerentemente con quanto sopra, dai membri del Gruppo per la Protezione dei Dati con la supervisione del DPO.

Il metodo utilizzato è coerente con il metodo di valutazione del rischio adottato per il Sistema di Gestione per la Qualità certificato UNI EN ISO 9001 e 13485, definito precisamente nella procedura "Metodologie di Analisi del Rischio" (P-D02) del Manuale Organizzativo Aziendale.

Si riporta di seguito l'estratto rilevante applicato ai trattamenti, come evidenziato nel Registro.

Il concetto di rischio è rappresentato dalla combinazione dei due seguenti elementi:

- la probabilità che avvenga il danno;
- le conseguenze di questo danno, cioè la gravità.

Sono quindi utilizzati i seguenti indici:

- Probabilità (P), probabilità che avvenga il danno (indipendentemente dalle misure di protezione);
- Gravità (G), gravità dell'impatto del danno sui diritti e le libertà delle persone;
- Rischio (R), definito come prodotto G x P, associato al singolo trattamento;
- Efficacia delle Misure di Protezione (E) adottate per abbattere il rischio: indice compreso tra 0 e 1 all'aumentare dell'efficacia
- Rischio Residuo (IRR) definito come prodotto tra R x (1-E).

L'indice di **probabilità** degli eventi considerati (compreso tra 1 e 5), è così definito: […Omissis…]

L'indice di gravità degli eventi considerati (compreso tra 1 e 5), è così definito: […Omissis…]

Sulla base del rischio come sopra definito (indice compreso tra 1 e 25), Fondazione CNAO ha stabilito i seguenti criteri di classificazione:

- Trascurabile, valore compreso tra […Omissis…]
- Basso, valore compreso tra […Omissis…]
- Medio, valore compreso tra […Omissis…]
- Inaccettabile, valore compreso tra […Omissis…]

Per quanto concerne il trattamento dei rischi, CNAO ha:

- Deciso di assumersi rischi trascurabili e bassi
- Identificato le azioni da attuare per gestire i rischi medi
- Deciso di non assumersi rischi inaccettabili

Per i trattamenti relativi alla ricerca clinica, la valutazione generale dei rischi è stata effettuata insieme agli altri trattamenti dal Gruppo per la Protezione dei Dati.

6.2 VALUTAZIONE DEL RISCHIO INIZIALE

L'esito della valutazione del rischio, indipendentemente dalle misure di protezione già in essere, per i due trattamenti individuati nell'ambito della ricerca clinica rileva rischi significativi, conseguenti a violazioni di riservatezza, integrità o disponibilità dei dati personali dei pazienti del CNAO arruolati all'interno di studi clinici, ed i seguenti possibili impatti:

- discriminazioni;
- danno di immagine;
- danni economici;
- danni alla salute.

[…Omissis…]

I rischi così individuati sono mitigati da Fondazione CNAO con misure di protezione classificate in due tipi:

- **Organizzative**: procedure, regole di comportamento ed istruzioni operative implementate in conformità al MOA (Modello Organizzativo Aziendale) (O).
- **Tecnologiche**: sistemi informativi e soluzioni automatizzate (T).

[…Omissis…]

A ciascun trattamento sono associate tutte le misure di protezione ad esso attribuibili. Il valore dell'efficacia sul trattamento è calcolato come media dell'efficacia delle misure applicabili.

Le misure di sicurezza implementate da CNAO sono progettate per gestire il più alto dei due rischi.

6.3 MISURE DI SICUREZZA

Per garantire la sicurezza e l'affidabilità dell'intero sistema, vengono adottate misure tecniche e organizzative conformi alla normativa vigente e alle regole interne che disciplinano la gestione e la conduzione degli studi clinici.

Dal punto di vista organizzativo, si fa riferimento alla procedura **P-P02**, che definisce in modo dettagliato i passi obbligatori da seguire, stabilendo:

- La documentazione da produrre in ciascuna fase dello studio;
- I soggetti coinvolti e le rispettive responsabilità;
- Le regole e i protocolli da rispettare per garantire il corretto svolgimento delle attività;
- I meccanismi di controllo e revisione per assicurare il rispetto delle disposizioni interne e normative.

La procedura **P-P02** è resa disponibile a tutti i professionisti coinvolti nelle attività di ricerca tramite il sito di Qualità.

Per quanto riguarda le misure tecnologiche, quelle applicate ai sistemi **in-house** sono descritte nel documento interno P-F01 (*Gestione del sistema informatico aziendale*), che definisce gli standard di protezione, le procedure di gestione e i controlli implementati per la salvaguardia dei dati e delle risorse IT e di seguito descritte in forma sintetica, con particolare attenzione alla gestione dei dati personali.

Nel rispetto del principio di sicurezza, informazioni relative ad eventuali aree di miglioramento sono state escluse dal presente estratto e potranno essere rese disponibili, ove richiesto, alle autorità competenti.

Sicurezza della infrastruttura in house

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Controllo degli accessi logici

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Conservazione e crittografia

[…Omissis…]	
VALUTAZIONE	**NON SUFFICIENTI**

Pseudonimizzazione

[…Omissis…]

VALUTAZIONE	**NON SUFFICIENTI**

Sicurezza dei canali informatici

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Sistemi di backup

[…Omissis…]	
VALUTAZIONE	**MIGLIORABILI**

Tracciabilità

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Sicurezza dei dispositivi di accesso (utente)

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Gestione delle vulnerabilità

[…Omissis…]	
VALUTAZIONE	**MIGLIORABILI**

Contratti con i responsabili del trattamento

[…Omissis…]	
VALUTAZIONE	**MIGLIORABILI**

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

[…Omissis…]	
VALUTAZIONE	**SUFFICIENTI**

Per quanto riguarda i **sistemi in cloud**, CNAO si affida a **Google Cloud Italy S.r.l.** per la messa a disposizione in cloud dei prodotti collegati a **Google Workspace** e **Google Cloud Platform**, che garantiscono elevati standard di sicurezza descritti e messi a disposizione del cliente nella seguente pagina: Sicurezza Google Cloud.

In particolare, Google adotta misure come la crittografia dei dati in transito e a riposo, l'autenticazione a più fattori, il monitoraggio costante delle attività e la protezione avanzata contro le minacce, per garantire la riservatezza, l'integrità e la disponibilità dei dati gestiti.

Per quanto riguarda la **conservazione digitale**, la **Fondazione** si avvale di **Argentea S.r.l** tramite il sistema **A4HealthCons**, che fornisce una soluzione di conservazione digitale a norma, assicurando l'integrità e l'autenticità dei documenti nel tempo. Le misure di sicurezza adottate da Argentea per garantire la protezione dei dati comprendono la protezione fisica e logica dei sistemi di conservazione, la gestione dei log di accesso e la duplicazione dei documenti. Per maggiori dettagli sulle misure di sicurezza implementate, è possibile consultare il manuale di conservazione di **A4HealthCons**: Manuale di Conservazione A4HealthCons.

I source documents della ricerca sono inviati in conservazione all'interno del fascicolo clinico del paziente, ne è pertanto coerentemente garantita la conservazione nel lungo periodo, l'univocità, l'integrità e la tracciabilità.

6.3.1 EFFICACIA DELLE MISURE DI SICUREZZA

Le misure tecniche ed organizzative implementate e brevemente descritte nel paragrafo precedente sono state valutate come sopra sintetizzato.

[…Omissis…]

6.4 ESITO DELLA VALUTAZIONE DEL RISCHIO RESIDUO

Applicato il metodo di valutazione dei rischi descritto, si ottiene per il trattamento in esame il seguente indice di rischio residuo "IRR", tenendo conto delle misure di sicurezza raccomandate per le due tipologie di trattamenti ed applicativi (in house o esternalizzati).

Date le misure di sicurezza già implementate (e potenziabili con le raccomandazioni del DPO) il rischio residuo ottenuto per tutti i parametri RID risulta basso o trascurabile.

ID	TRATTAMENTO	RISCHIO VIOLAZIONE	POSSIBILI IMPATTI SUI DIRITTI E LE LIBERTA' DELLE PERSONE	IRR
T11	Sperimentazione clinica non interventistica	riservatezza	discriminazioni, danno di immagine, danni economici	5,67
		integrità	nessun rischio rilevante per le persone	0,88
		disponibilità	nessun rischio rilevante per le persone	0,91
T12	Sperimentazione clinica interventistica	riservatezza	discriminazioni, danno di immagine, danni economici	5,67
		integrità	danno alla salute	4,39
		disponibilità	danno alla salute	4,54

Le **soluzioni adottate** per il rispetto dei principi fondamentali posti alla base della protezione dei dati e per far fronte ai rischi per le libertà e i diritti degli interessati **sono quindi considerate complessivamente accettabili**.

7 PARERE DEL DPO

La presente valutazione di impatto è redatta in conformità ai requisiti dell'articolo 35 del GDPR ed alla linea guida WP248 del European Data Protection Board e ne contiene tutti gli elementi essenziali:

- sono descritte la natura, l'ambito di applicazione, il contesto e le finalità del trattamento;
- sono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
- è fornita una descrizione funzionale del trattamento e l'organizzazione dispone di una apposita procedura dettagliata (P-P02);
- sono individuati gli asset ed i sistemi mediante i quali si effettuano i trattamenti;
- sono valutate necessità e proporzionalità;
- sono determinate le misure previste per garantire il rispetto del GDPR (principi base del trattamento, modalità di esercizio dei diritti degli interessati, rapporti con i responsabili del trattamento, eventuali garanzie riguardanti trattamenti internazionali);
- i rischi per i diritti e le libertà degli interessati sono analizzati, valutati e gestiti;
- l'origine, la natura, la particolarità e la gravità dei rischi vengono determinate dalla prospettiva degli interessati;
- sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- sono stimate la probabilità e la gravità;
- sono determinate le misure previste per gestire tali rischi.

La DPO è stata consultata. Non sono state raccolte le opinioni degli interessati perché la materia è troppo tecnica e gli interessati sono soggetti vulnerabili (pazienti oncologici).

Per quanto concerne le misure di protezione, il DPO rileva la necessità di portare a termine i progetti di potenziamento sul profilo della configurazione dei sistemi e della comunicazione con i destinatari […Omissis…]

La DPO di Fondazione CNAO

8 NORMATIVA DI RIFERIMENTO APPLICABILE AL PROCESSO

In questa sezione sono indicate le principali fonti normative e dottrinali applicabili al processo di Valutazione di Impatto in esame:

- World Medical Association. Dichiarazione di Helsinki – Principi etici per la ricerca biomedica che coinvolge gli esseri umani. 2013; art. 32.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) – e in particolare l'art.35, comma 3, lett. b).
- Regolamento (UE) n. 2014/536 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE, e in particolare artt. 1, 2, 28, 29, 56, 58 e cons. 29, 76.
- Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio - e in particolare artt. 1, 2, 63, 64, 65, 66, 72 e cons. 47, 67, 89
- Decreto 30 novembre 2021 del Ministero della Salute recante le 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 di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52.
- ICH Good Clinical Practice.
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research (adopted on 2 February 2021).
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" – e in particolare artt. 110 e 110-bis
- Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - n. 497 del 13 dicembre 2018
- Decreto Legislativo 5 giugno 1998, n. 204 "Disposizioni per il coordinamento, la programmazione e la valutazione della politica nazionale relativa alla ricerca scientifica e tecnologica, a norma dell'articolo 11, comma 1, lettera d), della legge 15 marzo 1997, n. 59"
- Decreto legislativo 30 dicembre 1992, n. 502 "Riordino della disciplina in materia di sanità, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421"
- Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza

- Faq del Garante per la Protezione dei dati personali "Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca"
- WP 248 – Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, nello specifico cap. III, B4.
- Provvedimento del Garante per la protezione dei dati personali, n. 467, del 11 ottobre 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, del Regolamento (UE) n. 2016/679, allegato I, pt. 6 e 10.
- Garante per la protezione dei dati personali – Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 (Registro dei provvedimenti n. 55 del 7 marzo 2019).
- Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679.
- Linee guida Linea Guida per la classificazione e conduzione degli studi osservazionali sui farmaci (det. AIFA 425/2024).
- Parere 3/2019 *"relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati"* dell'European Data Protection Board.
- EMA /INS/GCP/112288/2023 "*Guideline on computerised systems and electronic data in clinical trials*" – marzo 2023.