



MODELLO VALUTAZIONE DI IMPATTO DI:

**Progetto di Ricerca***AI-HOPE Lung cancer: building a predictive tool for metastatic lung cancer)***Compilatore:** Dott. Andrea Luciani e dott.ssa Liana Bevilacqua**Funzione:** Responsabile dell'Attività Progettuale**Fase 1: ANALISI DEL CONTESTO**

<b>Seleziona la categoria di interessati i cui dati personali sono trattati</b>
<p><input checked="" type="checkbox"/> <b>Pazienti</b></p> <p><input type="checkbox"/> Familiari dei Pazienti</p> <p><input type="checkbox"/> Altro _____</p>
<b>Per Ciascun soggetto interessato, elenca le categorie di dati strettamente necessari per condurre la ricerca scientifica</b>
<p>PAZIENTI:</p> <p><input checked="" type="checkbox"/> <b>Dati Anagrafici</b></p> <p><input checked="" type="checkbox"/> <b>Contatti (es. telefono/mail)</b></p> <p><input checked="" type="checkbox"/> <b>Immagini</b></p> <p><input checked="" type="checkbox"/> <b>Dati relativi alla salute</b></p> <p>Lo studio, denominato AI-HOPE, ha l'obiettivo di identificare variabili predittive e/o prognostiche per migliorare la risposta ai trattamenti standard per il carcinoma polmonare metastatico. E nello specifico sarà quello di identificare variabili che possano predire:</p> <ul style="list-style-type: none"><li>• Progressione precoce (entro 3 mesi dall'inizio del trattamento).</li><li>• Tossicità moderato-severa (con focus su tossicità polmonari).</li><li>• Lunga sopravvivenza (superiore alla mediana degli studi clinici).</li></ul> <p>Per i pazienti arruolati verranno raccolte queste variabili:</p> <ul style="list-style-type: none"><li>• Dati clinici (anagrafici, comorbidità, farmaci concomitanti, performance status, sintomi) pre-primi ciclo di terapia;</li><li>• Dati di andamento clinico (sopravvivenze, tossicità, trattamenti aggiuntivi) all'ultima visita di follow-up disponibile;</li><li>• Dati laboratoristici (conta emocromocitometrica, funzionalità epato-renale, indici di fase acuta) pre-primi ciclo di terapia e a tre mesi e/o in concomitanza della prima rivalutazione strumentale;</li><li>• Dati radiologici (dimensione del tumore primitivo, interessamento linfonodale, sedi e numero di metastasi, etc) e di radiomica (ove applicabile) pre-primi ciclo di terapia e a tre mesi e/o in concomitanza della prima rivalutazione strumentale;</li><li>• Dati di medicina nucleare acquisiti con PET-FDG pre-primi ciclo di terapia e, se disponibile, a tre mesi e/o in concomitanza della prima rivalutazione strumentale;</li><li>• Dati anatomo-patologici e di biologia molecolare (istologia, PD-L1, analisi stato mutazionale di EGFR, ALK, ROS1, BRAF, KRAS, RET, MET, NTRK) pre-primi ciclo di terapia</li></ul> <p>FAMILIARI:</p> <p><input type="checkbox"/> <b>Dati Anagrafici</b></p>


☐ Contatti (es. telefono/mail)

☐ Immagini

☐ Dati relativi alla salute

(Indicare i criteri per valutare il campione e le informazioni attese)

---



---

**Indicare i criteri di pseudo anonimizzazione che si intende applicare sui dati identificati dei pazienti/familiari oggetto di indagine.**

SI OSSERVERANNO I CRITERI DI PSEUDOANINIMIZZAZIONE DELL'ENTE PROMOTORE

---

**Tempi di conservazione stabiliti dal Massimario di scarto:**

Lo studio retrospettivo raccoglierà dati fino al primo semestre del 2024, mentre la fase prospettica si concluderà il 31 dicembre 2025. L'osservazione dei pazienti proseguirà fino a decesso o ritiro del consenso.

I dati sono conservati fino al termine dello studio e successivamente per il tempo previsto dalla normativa per la conservazione di dati di ricerca.

Alla fine del progetto, i dati saranno resi completamente anonimi o cancellati in conformità con le normative vigenti in materia di protezione dei dati (GDPR).

Questo ciclo garantisce la protezione della privacy e la sicurezza dei dati personali in ogni fase, rispettando i principi del GDPR

**Luogo di custodia dei dati**

☐ Server aziendale

☒ **Server/Archivi del Partner Promotore**
☐ Server di terza parte

☐ Archivio di /Servizio \_\_\_\_\_

**Rappresentare le categorie di soggetti interni all'organizzazione da autorizzare al trattamento dei dati:**

Personale incaricato e delegato dal Responsabile dello studio con i seguenti profili:

ONCOLOGI, INFERMIERI, RADIOLOGO, DATA MANAGER

**Elencare gli Enti/società Esterne Destinatarie (Registrare data e firma dell'Accordo con i Responsabili del Trattamento/Partners )**

ENTE PROMOTORE – IRCCS SAN RAFFAELE – Titolare Autonomo

#### Finalità che rendono necessario il trattamento dei dati:

Il trattamento dei dati nel contesto del protocollo AI-HOPE ha obiettivi chiaramente definiti. Lo scopo primario è sviluppare un algoritmo predittivo basato sull'intelligenza artificiale per individuare variabili che possano predire la risposta dei pazienti con carcinoma polmonare metastatico ai trattamenti immunoterapici e chemioterapici standard. Le variabili di interesse sono delineate con precisione, inclusi dati clinici, radiologici, laboratoristici e patologici.



Il protocollo delinea esplicitamente gli obiettivi di raccogliere e analizzare i dati dei pazienti al fine di sviluppare uno strumento di previsione che possa migliorare le decisioni terapeutiche in oncologia polmonare. Questo scopo è stato dichiarato sin dall'inizio del protocollo, descrivendo chiaramente l'uso della tecnologia di machine learning per analizzare variabili cliniche al fine di migliorare l'efficacia del trattamento oncologico. Inoltre, il protocollo fornisce dettagli sull'uso specifico dei dati raccolti e sull'integrazione con gli strumenti di machine learning, evidenziando come le informazioni saranno utilizzate.

Scopi legittimi:

Gli scopi del trattamento sono legittimi perché mirano a migliorare l'efficacia clinica e i risultati terapeutici per i pazienti affetti da carcinoma polmonare metastatico, rispettando i principi del Regolamento Generale sulla Protezione dei Dati (GDPR). Lo studio è condotto in conformità con i principi etici, seguendo le linee guida delle Buone Pratiche Cliniche e della Dichiarazione di Helsinki. Inoltre, la raccolta e il trattamento dei dati sono giustificati dall'interesse scientifico e clinico, e sono espressamente collegati alla ricerca medica e al miglioramento delle cure oncologiche.

Si precisa che i dati raccolti in questo progetto serviranno ad "addestrare" la machine learning descritta nello studio e che quindi l'intelligenza artificiale non avrà effetti diretti sui pazienti coinvolti nello studio

**a) Presupposti giuridici che rendono lecito il trattamento:**

**X Consenso dell'Interessato legittimare il trattamento dei dati dei pazienti che rientrano nella coorte prospettica.**

- ☐ Interesse pubblico Rilevante
- ☐ Soddisfazione di una norma di legge \_\_\_\_\_

**X Altro: Applicazione dell'art. 110 del D.lgs 196/2003 per i pazienti per la coorte retrospettiva.**

L'articolo 110 consente il trattamento di dati personali per ricerca scientifica **senza consenso** se il consenso è impossibile da ottenere o richiede uno sforzo sproporzionato. Nel caso della coorte retrospettiva di **AI-HOPE**, queste condizioni sono soddisfatte per diversi motivi:

- **Dati già raccolti:** lo studio utilizza dati clinici preesistenti, che sono stati originariamente raccolti per scopi clinici e diagnostici, e non per questa specifica ricerca.
- **Difficoltà di contatto con i pazienti:** Alcuni pazienti potrebbero essere **deceduti**, trasferiti o non più in contatto con le strutture sanitarie; il loro stato di salute potrebbe rendere difficile o inappropriato un contatto successivo.
- **Distorsione dei risultati:** richiedere il consenso solo a una parte della coorte (escludendo chi non può essere contattato) potrebbe introdurre un **bias di selezione**, compromettendo la validità scientifica dello studio.

Di conseguenza, l'impossibilità di ottenere il consenso senza uno sforzo sproporzionato giustifica l'applicazione dell'art. 110.

## **Fase 2 IDENTIFICAZIONE DEI TRATTAMENTI PREVISTI A RISCHIO**

**X trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato**

- ☐ trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto di avvalersi di un bene o di un servizio o di continuare ad essere parte di un contratto in essere
- ☐ trattamenti che prevedono un uso sistematico dei dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il



trattamento di identificativi univoci in grado di identificare gli utenti dei servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati.

**X trattamenti su larga scala di dati aventi carattere estremamente personale (es: vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale o la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato)**

**X trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)**

**X trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es: IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, etc.)**

- ☐ trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
- ☐ trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento
- ☐ trattamenti di dati sensibili o relativi a condanne penali
- ☐ trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

**X trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.**

### Fase 3: MISURE DI SICUREZZA ADOTTATE

#### A. DIRITTI IN MATERIA DI PRIVACY

DIRITTI DEGLI INTERESSATI
<i>Il progetto analizzato assicura il diritto alla rettifica dei dati</i>
<i>Il progetto analizzato assicura il tracciamento delle rettifiche eseguite</i>
<i>Il progetto analizzato assicura l'esportazione e portabilità dei dati in un formato di uso comune</i>
<i>Il progetto analizzato assicura la limitazione dell'accesso agli utenti se richiesto dall'interessato</i>
<i>Il progetto analizzato assicura la cancellazione definitiva dei dati di un utente</i>
<i>L'informativa è chiara ed accessibile agli interessati del trattamento analizzato ex art.13-14 del Reg. UE 2016/679</i>
<i>Il consenso. Dove acquisito, è documentabile e rintracciabile</i>
PERTINENZA E NECESSITA' DEI DATI
<i>Compilazione e acquisizione dei dati sono strettamente necessari e proporzionati alle finalità</i>
SOLO PER ARCHIVI DIGITALI: GESTIONE / HOSTING
<i>Il progetto analizzato assicura la gestione dei dati nell'Unione Europea</i>

**B. RISERVATEZZA DEI DATI**

<b>CONTROLLO DEGLI ACCESSI E AUTENTICAZIONE ALLE RISORSE INFORMATICHE COINVOLTE NEL PROGETTO ANALIZZATO (es. PC, Server, Software ecc)</b>
<i>L'accesso è consentito tramite username e password personale</i>
<i>Utilizzo di password alfanumeriche di almeno 8 caratteri</i>
<i>Si attiva il blocco automatico in caso di tentativi falliti di accesso multipli</i>
<i>È impostata una password provvisoria per il primo accesso che viene cambiata automaticamente dall'operatore</i>
<i>E' previsto il Logout dell'utente dopo un periodo di inattività</i>
<i>E' impedita l'adozione di un account utente comune (consentito solo tra utenti con uguale ruolo e responsabilità)</i>
<i>Sono documentate e condivise con il personale le politiche di gestione della password</i>
<i>Accesso al sistema IT è eseguito solo da sistemi e terminali pre-autorizzati</i>
<i>I PC sono dotati di antivirus</i>
<i>L'aggiornamento del sistema antivirus avviene in modo centralizzato</i>
<i>La rete è protetta da firewall</i>
<i>Il personale è formato rispetto ai rischi informatici</i>
<i>In caso di dimissioni del dipendente/ricercatore il suo account viene sospeso e/o rimosso</i>
<i>Lo screensaver con protezione di PW si attiva automaticamente sui PC</i>

**C. INTEGRITA'**

<b>PROCEDURE E PROTOCOLLI</b>
<i>Sono definiti i criteri di controllo della correttezza e completezza dei dati personali, anche in modalità non automatica</i>
<i>Sono previste forme di verifica a campione o regolari sulla correttezza e completezza dei dati personali</i>

**D. DISPONIBILITA'**

<b>LOCALI IN CUI SONO COLLOCATI ARCHIVI, PC e SERVER</b>
<i>I PC/server sono sollevati da terra</i>
<i>Nei locali sono disposte misure antincendio adeguate e periodicamente controllate</i>
<i>Gli impianti elettrici e di climatizzazione sono periodicamente controllati</i>
<i>I PC/server sono dotati di gruppi di continuità</i>
<b>PC IN DOTAZIONE</b>
<i>Esiste un piano di manutenzione dei PC dato in dotazione</i>



<i>Sono previsti e condivisi codici comportamentali per il corretto utilizzo dei PC o dispositivi affidati</i>
<b>CARTELLE DEL SERVER e/O FASCICOLI CARTACEI</b>
<i>Le cartelle del server o fascicoli cartacei sono organizzati secondo criteri comuni condivisi</i>
<i>Esiste sempre una copia di sicurezza dei documenti cartacei o digitali prodotti</i>
<b>SOLO PER SOFTWARE/GESTIONALI UTILIZZATO PER L'ESTRAZIONE E CARICAMENTO DEI DATI</b>
<i>È previsto un contratto di assistenza per manutenzioni ordinarie e straordinarie di software e gestionali</i>
<b>SOLO PER ARCHIVI DIGITALI: BACK UPS e PROCEDURE DI BUSINESS CONTINUITY</b>
<i>Si riscontra un adeguato livello di protezione fisica e ambientale per i backup</i>
<i>E' previsto il monitoraggio della corretta esecuzione dei backup per garantire la sicurezza</i>
<i>E' prevista una regolare esecuzione di backup completi (Esecuzione almeno giornaliera dei backup incrementali)</i>
<i>E' previsto il regolare test delle procedure di backup</i>

**E. MISURE SICUREZZA PIATTAFORMA REDCAP AZIENDALE**

<b>MISURE ADOTTATE</b>
<i>Accesso consentito tramite username e password personale</i>
<i>Utilizzo di password alfanumeriche</i>
<i>Utilizzo di password di almeno 8 caratteri</i>
<i>Blocco automatico in caso di tentativi falliti di accesso multipli</i>
<i>Impostazione di una password provvisoria per il primo accesso</i>
<i>Cambio automatico della password da parte dell'operatore</i>
<i>Logout dell'utente dopo un periodo di inattività</i>
<i>Implementazione di un sistema di controllo degli accessi per gli utenti che accedono al sistema IT</i>
<i>Evitare l'uso di account utente comune (consentito solo tra utenti con uguale ruolo e responsabilità)</i>
<i>Definizione e documentazione di una policy specifica per gestione della password</i>
<i>Memorizzazione delle password in una forma "hash"</i>
<i>Necessaria registrazione delle azioni degli amministratori e operatori di sistemi</i>
<i>Accesso al sistema IT eseguito solo da sistemi e terminali pre-autorizzati</i>



## GENERAZIONE E CONTROLLO FILE DI LOG

MISURE ADOTTATE
Tracciamento delle operazioni in un file di log
Facile esportazione dei log dall'ADS
Conservazione dei log per almeno 6 mesi
Creazione file di log per ogni sistema/applicazione utilizzata per trattamento dati
File di log contrassegnati da data e ora
Protezione file di log da manomissioni e accessi non autorizzati
Creazione file di log e report sullo stato del sistema da parte del sistema di monitoraggio

## Fase 4: CALCOLO DEL RISCHIO

	TUTELA DEI DIRITTI	RISERVATEZZA	INTEGRITA'	DISPONIBILITA'
Misure di controllo	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input type="checkbox"/> ADEGUATE <input checked="" type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE
<b>PROBABILITÀ DI ACCADIMENTO DI INCIDENTI PRIVACY</b> (Identifica un valore da 1 a 3 sulla base dell'adeguatezza delle misure presenti)	1	1	1	2
<b>IMPATTO STIMATO SULL'INTERESSATO</b> (Identifica un valore da 1 a 3 sulla base delle conseguenze stimate sui diritti e libertà dell'interessato)	3	2	3	1
<b>RISCHIO</b> (Calcola il rischio moltiplicando il coefficiente assegnato all'impatto e alla probabilità)	3	2	3	2

Attenzione: Prima di procedere alla compilazione consulta la legenda a seguire.

**Legenda Adeguatezza delle Misure di Controllo:**

- ☐ ADEGUATE (Più del 50% delle misure attese applicabili sono soddisfatte)
- ☐ PARZIALMENTE ADEGUATE (Sono state applicate tra il 50% e il 25% delle misure attese applicabili)
- ☐ NON ADEGUATE (È stato applicato al massimo il 25% delle misure attese applicabili)

**Attenzione: Nel calcolo delle misure soddisfatte sono da sottrarre le misure N/A.**

**Legenda Probabilità:**

- 1 – Le misure di controllo sono ADEGUATE e tali da garantire la riservatezza, integrità, disponibilità e liceità dei dati personali raccolti
- 2 – Le misure di controllo sono PARZIALMENTE ADEGUATE in termini di riservatezza, integrità, disponibilità e liceità dei dati personali raccolti
- 3 – Le misure di controllo NON SONO ADEGUATE sul piano della riservatezza, integrità, disponibilità e liceità dei dati personali raccolti

**Legenda Impatto:**

- 1 – L'interessato (es. paziente, fornitore, lavoratore) non subisce in caso di incidente privacy **nessun effetto** rispetto ai diritti, agli accordi/prestazioni attese o danno alla reputazione, danno morale e/o economico
- 2 – L'interessato potrebbe essere oggetto di un **temporaneo disservizio sanato da procedure alternative** oppure è **oggetto di un controllo accessorio** (es. replica della prestazione ricevuta; ritardo nell'erogazione di una prestazione; perdita temporanea del controllo dei propri dati)
- 3 – L'interessato **potrebbe subire qualche forma di discriminazione, penalizzazione o sanzione** (es. perdite finanziarie, perdita del lavoro, pregiudizio alla reputazione, usurpazione dell'identità, danno alla salute)

**Legenda Rischio**

IMPATTO	3	6	9
	2	4	6
	1	2	3
PROBABILITA'			

VERDE: RISCHIO BASSO. Progetto sicuro

GIALLO: RISCHIO MEDIO. Progetto da tenere sotto controllo rafforzando le misure di sicurezza.

ROSSO: RISCHIO ALTO. Progetto non sicuro

Fase 5: PARERE DEL DPO

- ☐ **Necessario**
- ☒ **Non necessario**

(Allegare il Parere del DPO, dove richiesto)

**Data**

\_\_\_\_\_

**Firma**

\_\_\_\_\_