



La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Essa mette dunque a disposizione:

- una descrizione sistematica del trattamento;
- la esplicitazione delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure tecniche e organizzative che il titolare ritiene di dover adottare allo scopo di mitigare tali rischi.

La DPIA è redatta dal preposto al trattamento e oggetto di valutazione del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO

Denominazione del trattamento

Tumore Fibroso Solitario: fattori prognostici fra valutazione istopatologica e nuovi approcci di diagnostica biomolecolare

Indicare lo scopo pratico del trattamento

Studio finalizzato alla individuazione di fattori prognostici nei pazienti affetti da tumore fibroso solitario, tumore raro, in cui permane una difficoltà, con i criteri dell'istopatologia tradizionale, nel definire il grado di aggressività del tumore e conseguentemente nel valutare le migliori opzioni terapeutiche (solo chirurgia oppure terapie adiuvanti associate).

Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato

Le tipologie di informazioni raccolte ed utilizzate comprenderanno i dati anagrafici, la diagnosi oncologica con relativa data e stadiazione, la sede e le caratteristiche del tumore (dimensioni, localizzazione sovra- o sotto-fasciale), i trattamenti effettuati, lo status oncologico al follow-up, i dati molecolari relativi alle indagini previste dallo studio sui campioni tissutali, patologie concomitanti, data diagnosi del tumore. Nel database, associati al codice di pseudonimizzazione, saranno archiviate, oltre ai dati sopra indicati, le informazioni molecolari provenienti dalle analisi previste dallo studio

Indicare le tipologie di persone fisiche interessate al trattamento

Pazienti sottoposti a trattamento per tumore fibroso solitario delle parti molli presso la SOD Ortopedia Oncologica e Ricostruttiva dell'AOU Careggi dal 2002 al 2020

Indicare i soggetti interni (anche per categoria) che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento

I soggetti che parteciperanno al trattamento dei dati saranno Dirigenti Medici e/o Dottori/Dottoresse in Biologia o Biotecnologie, afferenti in entrambi i casi all'Azienda Ospedaliero-Universitaria di Careggi (con rapporto a tempo indeterminato o determinato), espressamente designati ed autorizzati, nonché istruiti sul trattamento.



Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento e se questi siano state adeguatamente istruiti sul trattamento
///

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). È preferibile allegare un diagramma di flusso, altrimenti occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori
Tutti i dati raccolti convergeranno in un database comune. Le informazioni generali, cliniche e molecolari di ogni paziente saranno collezionate all'interno del database, implementando specifiche strategie per mantenere un adeguato livello di privacy. In particolare, per assicurare una adeguata sicurezza del database e la possibilità di tracciare gli accessi, il database sarà costruito e gestito attraverso il programma RedCap sito sul server aziendale AOU Careggi, con accesso tramite utente registrato e password e con tracciatura di ogni accesso. Per le analisi statistiche sarà creato un file temporaneo Excel, che dopo l'utilizzo sarà cancellato. I risultati saranno presentati in forma aggregata.

Indicare dove vengono archiviati i dati

Come su indicato, i dati saranno archiviati sul server aziendale dell'AOU Careggi, con le conseguenti tutele e limitazioni e tracciamento degli accessi, utilizzando il software Redcap.

Indicare se i dati sono trasferiti (si/no) ed eventualmente dove: (fuori dall'Azienda, fuori dall'Italia, fuori dall'Unione Europea)

NO

PRINCIPI FONDAMENTALI

Limitazione delle finalità: indicare la base giuridica del trattamento (cioè la finalità, quale prevista dal Regolamento UE 2016/679)

Il trattamento dei dati degli interessati che sarà possibile informare si basa sul consenso ai sensi dell'art. 9 par. 2 lettera a) del Regolamento UE 2016/679 e dell'art. 110 del D.Lgs. 30 giugno 2003 n. 196.
Per gli interessati che non sarà possibile informare e per i quali non sarà possibile ottenere il consenso, in quanto risultino essere al momento dell'arruolamento nello studio deceduti o comunque non contattabili (all'esito di ogni ragionevole sforzo compiuto per contattarli, anche attraverso 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), si procederà secondo le modalità di cui all'art. 110 comma 1 secondo periodo del D.Lgs. 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali, ovvero mediante sottoposizione del protocollo di studio a consultazione preventiva dell'Autorità Garante per la protezione dei dati personali.

Minimizzazione dei dati: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati

Saranno raccolti solo i dati indispensabili per lo studio, come descritti nel protocollo

Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati

I dati (pseudonimizzati) saranno conservati per un periodo non superiore a quello necessario per le finalità dello studio per i quali sono stati raccolti – stimabile in 7 (sette) anni dalla conclusione dello studio. Dato



atto che, per gli studi osservazionali, la valenza normativa dei termini di conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, è, se certo non assente, comunque alquanto indiretta e non immediatamente prescrittiva, il Titolare del trattamento ha ritenuto opportuno, nella prospettiva della accountability, applicare a questo studio osservazionale il termine dei 7 anni già previsto dal D.Lgs. 6 novembre 2007, n. 200

Esattezza dei dati: indicare le misure individuate per aggiornare, correggere o cancellare i dati che risultano non esatti in riferimento alla finalità per la quale sono trattati

All'atto dell'inserimento nel database, verrà effettuata una doppia verifica del dato estratto dalla documentazione clinica

Integrità e riservatezza dei dati: indicare le misure tecniche ed organizzative adottate per garantire la sicurezza dei dati rispetto a trattamenti non autorizzati o illeciti, perdita, distruzione o danni accidentali

La sicurezza dei dati è assicurata dall'utilizzo del software Redcap sul server aziendale, con tracciamento accessi e modifiche

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità

SI, con numero/codice progressivo, non identificativo. La chiave di decifrazione della pseudonimizzazione verrà conservata in modo riservato.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità

NO

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità

SI, quando i dati vengono aggregati nell'analisi statistica (pur rimanendo nel database il dato pseudonimizzato)

Indicare se i dati sono fisicamente suddivisi in archivi dati separati (partimentazione)

NO

Indicare con quali misure e cautele viene effettuato il trasferimento dei dati

Si accede a Redcap con profili di autorizzazione specifici

Indicare i criteri di profilazione per l'accesso ai dati

Viene profilato il gruppo di sperimentazione in scrittura e lettura

Indicare se gli accessi sono tracciati

SI, su Redcap

Indicare con quale frequenza viene effettuato il backup dei dati

In automatico, secondo il protocollo del software Redcap aziendale AOU Careggi

Indicare se il sistema prevede misure contro virus e malware

SI (server aziendale AOU-Careggi)



Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti

NO

DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento

Per i pazienti non contattabili o defunti (per questi ultimi, più precisamente, per i soggetti di cui all'art. 2-terdecies del D.Lgs. 196/2003), l'informativa sarà resa disponibile sul sito istituzionale.

Per i pazienti contattabili: vedi sotto

Ove applicabile: indicare come è acquisito il consenso degli interessati

Il consenso viene acquisito mediante colloquio e firma di specifico modulo di consenso

Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come

NON APPLICABILE (non vi sono soggetti esterni titolari)

Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente

NON APPLICABILE

GESTIONE DEI RISCHI

ACCESSO ILLEGITTIMO AI DATI

Sebbene la gravità del rischio possa essere considerata di medio livello, vista la specificità e le caratteristiche dei dati sensibili trattati, la probabilità del rischio si ritiene trascurabile.

I dati sono infatti pseudonimizzati e separati dalle informazioni anagrafiche dei pazienti; il server che ospita il database è accessibile esclusivamente attraverso il protocollo https (TLS) con esclusione di ogni accesso di altro tipo (SMB, FTP o altri).

Gli accessi sistemistici di servizio (per manutenzione o aggiornamenti software) sono consentiti solo attraverso protocolli criptati (ssh o simili) e soltanto da rete intranet AOUC. Eventuali necessità di accessi da internet sono veicolati attraverso VPN.

Le credenziali amministrative sono in possesso del solo personale interno autorizzato.

Le credenziali di gestione dell'applicativo sono personali e rilasciate ai soli dipendenti autorizzati che sono stati istruiti riguardo la loro corretta custodia.

MODIFICHE INDESIDERATE DEI DATI

La probabilità del rischio di modifica indesiderata dei dati può essere ritenuta trascurabile, anche alla luce delle misure pianificate. La gravità del rischio è stimata di medio livello.

I dati vengono sottoposti a backup giornaliero, con possibilità di rapido *restore* in caso si verifichi una modifica indesiderata.

L'accesso in scrittura ai dati è riservato a selezionati utenti, ed avviene attraverso interfacce che minimizzano la probabilità di errore.



PERDITA DEI DATI

La probabilità di perdita dei dati è estremamente **bassa**, mentre l'eventuale danno sarebbe molto elevato. La stima considera le strutture hardware ridondate sulle quali si fonda il sistema, le procedure di backup sistematico e la resilienza intrinseca del data center che ospita l'applicativo.

Per gli eventuali *data loss* causati da operatori infedeli, valgono le considerazioni dei punti precedenti.



VALUTAZIONE DEL PREPOSTO AL TRATTAMENTO

(nome/cognome)

Dr. Guido Scoccianti

FIRMA 	Data 16/06/2023
--	------------------------

VALUTAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

(nome/cognome)

Paolo Tagliaferri

FIRMA 	Data 18/06/2023
---	------------------------

PIANO D'AZIONE (misure da implementare, se valutato necessario, per minimizzare i rischi e garantire misure di maggior tutela degli interessati)

PRINCIPI FONDAMENTALI

...

DIRITTI DEGLI INTERESSATI

...

GESTIONE DEI RISCHI

...